Information Security Policies

V 2.5

www.gradleaders.com
614.791.9000

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Everyone recognizes that the highway system and motor vehicles are essential to commerce. But people are only recently coming to appreciate how information systems made up of computers and networks are another infrastructure essential to commerce. In recognition of the critical role that information systems play in GradLeaders USA, LLC. business activities, this policy defines the rules of the road and other requirements necessary for the secure and reliable operation of the GradLeaders USA, LLC. information systems infrastructure.

Just as every driver has a role to play in the orderly and safe operation of the transportation infrastructure, so too are there information security roles and duties for every worker at GradLeaders USA, LLC. For example, it is a driver's duty to report accidents, and it is a worker's duty to report information security problems. Just as car manufacturers are required to provide safety belts with vehicles, system designers at GradLeaders USA, LLC. are required to include necessary security measures such as user access restrictions based on the need to know.

These policies also define baseline control measures that everyone at GradLeaders USA, LLC. is expected to be familiar with and to consistently follow. Sometimes called standard of due care controls, these security measures are the minimum required to prevent a variety of different problems including: fraud and embezzlement, industrial espionage, sabotage, errors and omissions, and system unavailability. These policies also define the minimum controls necessary to prevent legal problems such as allegations of negligence, breach of fiduciary duty, or privacy violation. This policy document details both reasonable and practical ways for all of us at GradLeaders USA, LLC. to prevent unnecessary losses.

GradLeaders USA, LLC. critically depends on continued customer confidence. This confidence has been gradually increased and is the result of many years of dedicated effort on the part of GradLeaders USA, LLC. employees. While it is slow to grow, this confidence can be rapidly lost due to problems such as hacker intrusions causing system outages. The trust that customers have in GradLeaders USA, LLC. is a competitive advantage that must be nurtured and grown with efforts such as this information security initiative.

Introduction

Critical Business Function—Information and information systems are necessary for the performance of just about every essential activity at GradLeaders USA, LLC. If there were to be a serious security problem with this information or these information systems, GradLeaders USA, LLC. could suffer serious consequences including lost customers, reduced revenues, and degraded reputation. As a result, information security now must be a critical part of the GradLeaders USA, LLC. business environment.

Supporting Business Objectives—This information security policy document has been prepared to ensure that GradLeaders USA, LLC. is able to support further growth of the business, and ensure a consistently high level of customer, employee, and business-partner service. This document is also intended to support the organization’s reputation for high-integrity and high-quality business dealings. Because prevention of security problems is considerably less expensive than correction and recovery, this document will help reduce costs in the long run.

Consistent Compliance Essential—A single unauthorized exception to security measures can jeopardize other users, the entire organization, and even outside organizations such as business partners. The interconnected nature of information systems requires that all workers observe a minimum level of security. This document defines that minimum level of due care. In some cases, these requirements will conflict with other objectives such as improved efficiency and minimized costs. Top management has examined these trade-offs and has decided that the minimum requirements defined in this document are appropriate for all workers at GradLeaders USA, LLC. As a condition of continued employment, all workers, employees, contractors, consultants, and temporaries, must consistently observe the requirements set forth in this document.

Team Effort Required—The tools available in the information security field are relatively unsophisticated. Many of the needed tasks cannot be achieved with products now on the market. This means that users at GradLeaders USA, LLC. must step in and play an important role in the information security area. Now that information and information systems are distributed to the office desktop, and are used in remote locations, the worker's role has become an essential part of information security. Information security is no longer the exclusive domain of the Information Systems department. Information security is now a team effort requiring the participation of every worker who comes into contact with GradLeaders USA, LLC. information or information systems.

Information Ownership

New Centrality Of Information—Information is no longer simply something that supports the provision of a product or service. Information is a critical and integral part of the products and services that GradLeaders USA, LLC. provides. The new centrality of information necessitates the establishment of new roles and responsibilities to properly manage and protect it. To this end, this policy defines the information security roles and responsibilities of Owners, Custodians, and users. Information security can no longer be a concern of technical specialists alone. A large team of individuals must address it. This team is made up of every GradLeaders USA, LLC. worker who comes into contact with GradLeaders USA, LLC. information or information systems.

Policy Scope And Applicability—This policy applies to the handling of all GradLeaders USA, LLC. production information, regardless of the origin of this information. Production information is information routinely used to perform important business activities or routinely used to support management decision making. This policy applies despite what information handling technology is used, where the information resides, how the information is employed to meet business needs, and which users have access to the information. This policy applies to all GradLeaders USA, LLC. business units and all third parties performing business on behalf of GradLeaders USA, LLC.

Roles and Responsibilities Of Owners—Information Owners are senior business unit managers with the authority for acquiring, creating, and maintaining information and information systems within their assigned area of control. Owners are responsible for categorizing the information for which they have been designated an Owner using the classifications defined in the Data Classification Policy. To assist with contingency planning efforts, Owners also are responsible for categorizing information, or specific application systems, according to a criticality scale defined by the Information Security department. Owners are responsible for authorizing user access to information based on the need to know. Designated information Owners are responsible for establishing and updating specific written policies regarding the categories of people who will be granted permission to access information. As needed, these policies must specify limitations on the use of this information by those to whom access has been granted. The Information Security department will provide Owners with training, reference material, and consulting assistance so that they may appropriately make these and related decisions and distinctions. Owners also must make decisions about the permissible uses of information including relevant business rules. Owners are responsible for choosing appropriate information systems, and relevant controls for information handled by these systems, consistent with policies and standards issued by the Information Security department. For example, Owners must define the validation rules used to verify the correctness and acceptability of input data. These validation rules and other controls for protecting information must be formally approved in writing by the relevant Owner before major modifications can be made to production application systems. Owners must understand the uses and risks associated with the information for which they are accountable. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security-related control deficiencies pertaining to the information for which they are the designated Owner.

Roles And Responsibilities Of Custodians—Information Custodians are individuals, often staff within the Information Systems department or local department system administrators, in physical or logical possession of information from Owners. Custodians are charged with the provision of information systems services consistent with the instructions of

Owners, including information security measures such as encryption. Using physical and logical access control systems, Custodians must protect the information in their possession from unauthorized distribution, access, alteration, destruction, or usage. Custodians also are responsible for providing and administering general controls such as backup and recovery systems consistent with the policies and standards issued by the Information Security department. Custodians are responsible for establishing, monitoring, and operating information systems in a manner consistent with policies and standards issued by the Information Security department. Custodians must not change the production information in their possession unless they have received explicit and temporary permission from either the Owner or an authorized user.

Roles and Responsibilities Of Users—Information users are individuals who have been granted explicit authorization to access, modify, delete, or utilize information by the relevant Owner. Users must use the information only for the purposes specifically approved by the Owner. Users are not permitted to make additional copies of, or otherwise reproduce or disseminate sensitive information unless the Owner has expressly agreed. Users also must comply with all security measures defined by the Owner, implemented by the Custodian, or defined by the Information Security department. Users must additionally refrain from disclosing information in their possession, unless it has been designated as Public, without obtaining permission from the Owner. Users must report to the Information Security department all situations where they believe an information security vulnerability or violation may exist. Users of personal computers have special responsibilities, for example relating to backups and virus screening, that are defined in the Personal Computer Security Policy.

Multiple Roles And Responsibilities—It is likely that certain individuals will act in multiple capacities with respect to certain types of information. For example, an employee may be the creator of a new type of production information that is stored in a desktop personal computer. In this case, the employee must, at least temporarily, act in the capacity of Owner, Custodian, and user. To achieve a more secure operating environment, separate individuals must perform the roles of Owner, Custodian, and user wherever production information has more than one user. Creators of new types of production information must promptly inform the Information Systems Architecture group within the Information Technology department so that appropriate roles and responsibilities may be established and maintained.

Designating Owners—If there are several potential information Owners, the chief information officer must assign ownership responsibility to the senior manager of the business unit that makes the greatest use of the information. When acting in his or her capacity of Owner, this individual must take into consideration the needs and interests of other stakeholders who rely upon or have an interest in the information. With the exception of operational computer and network information, managers in the Information Systems department must not be Owners for any information. An Owner's roles and responsibilities may be delegated to any full-time manager in the Owner's business unit. An Owner's roles and responsibilities may not be assigned or delegated to contractors, consultants, or individuals at outsourcing organizations or external service bureaus.

Designating Custodians—Management must specifically assign responsibility for the control measures protecting every major production type of information. Owners are responsible for identifying all those individuals who are in possession of the information for which they are the designated Owner. These individuals by default become Custodians. Although special care must be taken to clearly specify security-related roles and responsibilities when outsiders are involved, it is permissible for Custodians to be contractors, consultants, or individuals at outsourcing organizations or external service bureaus.

Designating Users—Users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements, such as non-disclosure agreements, have been made. All users must be known to and authorized by Owners. The security-relevant activities of all users must be tracked and logged by Custodians. Users must always be specific individuals. Users must not be defined as departments, project teams, or other groups.

Changes In Status—The individuals who play the roles of information Owners, Custodians, and users will change on a regular basis. These changes in worker status must be communicated to the Information Security department. Custodians must maintain access control systems so that previously-provided user privileges are no longer provided whenever there has been a user status change. When a Custodian has a change in status, it is the responsibility of the Owner to promptly

assign a new Custodian, and to assist the new Custodian with the assumption of tasks previously performed by the former Custodian, including necessary training. When an Owner has a change in status, it is the chief information officer's responsibility to promptly designate a new Owner.

Handling Of Information Following Status Changes—Users who change their status must leave all production information with their immediate manager. Soon after a user has a change of status, both computer-resident files and paper files must be reviewed by the user's immediate manager to determine who should be given possession of the files, or the appropriate methods to be used for file disposal or destruction. The manager must promptly reassign the user's duties and specifically delegate responsibility for information formerly in the user's possession. It is this manager's responsibility to train the new user so that the new user is able to fully perform the tasks previously performed by the former user. It is this manager's responsibility that the new user become acquainted with the relationships that the previous user had with both insiders and outsiders, and become acquainted with all pending transactions and incomplete projects handled by the previous user.

Externally-Supplied Information—In the course of normal business activities, GradLeaders USA, LLC. often takes possession of third-party sensitive information. Whenever a non-disclosure agreement (NDA) has been signed, an internal GradLeaders USA, LLC. Owner must be assigned for information so received. The manager of the business unit utilizing the information is ordinarily designated as the Owner. The Owner must promptly report the existence of this third-party information to the Information Architecture group within the Information Technology department. This third-party information must be labelled with the appropriate data classification category and treated as though it was GradLeaders USA, LLC. internal information with the same classification. The roles and responsibilities for Custodians and users are also relevant to externally-supplied information.

System of Record—Each Owner must designate a system of record that will serve as the most authoritative copy of the information under his or her care. Updates to this information must be made to the system of record before or at the same time that updates are made to other systems containing this information. It is the Owner's responsibility to ensure that all production copies of the information for which he or she is the designated Owner are maintained with appropriate controls to ensure a reasonable degree of information accuracy, timeliness, and integrity.

Risk Acceptance Process—In rare circumstances, exceptions to information security policies and standards will be permitted if the information Owner, the director of the Information Security department, and the chief information officer have all signed a properly completed risk acceptance form. In the absence of such management approval reflected on a risk acceptance form, all Owners, Custodians, and users must consistently observe relevant GradLeaders USA, LLC. information security policies and standards.

Notifications Of Loss Or Disclosure—If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, its Owner and the director of the Information Security department must be notified immediately.

Data Classification

Overview

Worker Responsibility—Every worker who has access to GradLeaders USA, LLC. information or information systems has an important information security role in the organization. For example, each one of these workers is personally responsible for the protection of information that has been entrusted to their care. All workers who come into contact with sensitive GradLeaders USA, LLC. internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily GradLeaders USA, LLC. business activities. Sensitive information is either Confidential or Secret information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, workers are expected to apply and extend these concepts to fit the

needs of day-to-day operations. This document provides a conceptual model for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

Addresses Major Risks—The GradLeaders USA, LLC. data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect GradLeaders USA, LLC. information from unauthorized disclosure, use, modification, and deletion.

Consistent Approach Required—A single lapse in information security can have significant long-term consequences. Consistent use of this data classification system is essential if sensitive information is to be adequately protected. Without the consistent use of this data classification system, GradLeaders USA, LLC. unduly risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage. This policy consistently protects sensitive information no matter what form it takes, what technology is used to process it, who handles it, where the information may be located, and in what stage of its life cycle the information may be.

Applicable Information—This data classification policy is applicable to all information in the possession or under the control of GradLeaders USA, LLC. For example, Confidential information entrusted to GradLeaders USA, LLC. by customers, business partners, suppliers, and other third parties must be protected with this data classification policy. Workers are expected to protect third-party information with the same care that they protect GradLeaders USA, LLC. information. No distinctions between the words "data," "information," "knowledge," and "wisdom" are made for purposes of this policy.

Trade Secrets—One special type of sensitive information is called a Trade Secret. Trade Secrets are a type of proprietary information that gives GradLeaders USA, LLC. competitive advantage in some manner. This document covers Trade Secrets, all of which need to be separately designated. Trade Secrets must be identified as such prior to being disclosed to any worker. By default, all Trade Secrets are classified as Secret information. The GradLeaders USA, LLC. chief operating officer is the only person authorized to designate any GradLeaders USA, LLC. information as a Trade Secret.

Access Control

Need to Know—Every one of the policy requirements set forth in this document are based on the concept of need to know. If a worker is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information. This principle applies to private employee information such as medical histories, just as it applies to proprietary corporate information such as plans for a new product.

System Access Controls—Access to all GradLeaders USA, LLC. sensitive computer-resident information must be protected by access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. Whatever technology is employed, access must be controlled for each individual based on that individual's need to know. The notion of the need to know includes not only viewing information, but other privileges such as modifying information or using information to complete a transaction.

Access Granting Decisions—Access to GradLeaders USA, LLC. sensitive information must be provided only after the written authorization of the information Owner has been obtained. Custodians of the involved information must refer all requests for access to the relevant Owners or their delegates. Standard templates of system privileges are defined for all job titles, and Owners approve these privileges in advance. Special needs for other access privileges will be dealt with on a request-by-request basis.

Classification Labels

Owners And Production Information—All production information types possessed by or used by a particular organizational unit within GradLeaders USA, LLC. must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the GradLeaders USA, LLC. management team who act as stewards, and who supervise the ways in which certain types of information are used and protected .

SECRET—This classification label applies to the most sensitive business information that is intended for use strictly within GradLeaders USA, LLC. Its unauthorized disclosure could seriously and adversely impact GradLeaders USA, LLC., its customers, its business partners, and its suppliers. Examples include corporate level strategic plans, strategy memos, reports on breakthrough new product research, and Trade Secrets such as certain computer programs.

CONFIDENTIAL—This classification label applies to less-sensitive business information that is intended for use within GradLeaders USA, LLC. Its unauthorized disclosure could adversely impact GradLeaders USA, LLC. or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally-generated market research, computer passwords, identity token personal identification numbers, and internal audit reports.

FOR INTERNAL USE ONLY—This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact GradLeaders USA, LLC. or its employees, suppliers, business partners, or its customers. Examples include the GradLeaders USA, LLC. telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.

PUBLIC—This classification applies to information that has been approved by GradLeaders USA, LLC. management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Other Labels—GradLeaders USA, LLC. department or division-specific data classification labels are permissible, but must be consistent with and supplemental to the GradLeaders USA, LLC. data classification system. These supplementary labels might for example include the use of words like “Private” or “Financial.”

Owners And Access Decisions—Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. Owners must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

Labeling

Consistent Classification Labeling—If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labeled with an appropriate data classification designation. Such markings must appear on all manifestations of the information, such as hard copies, floppy disks, and CD-ROMs. Workers must not remove or change data classification system labels for sensitive information unless the permission of the Owner has been obtained.

What Gets Labeled—The vast majority of GradLeaders USA, LLC. information falls into the Internal Use Only category. For this reason, it is not necessary to apply a label to Internal Use Only information. Information without a label is by default classified as Internal Use Only.

Labels Believed To Be Incorrect—If the recipient of GradLeaders USA, LLC. internal information believes that the data classification label accompanying this information is incorrect, the recipient must protect the information in a manner consistent with the more stringent of the two possible classification labels. Before using this information or distributing it to any other party, such a recipient must check with the information Owner to ensure that the label currently applied to the information is correct.

Information Collections—Workers who create or update a collection of information are responsible for choosing an appropriate data classification label for the new collection. This label must be consistent with the decisions made by the relevant Owners and generally should be the most restricted classification level found in the collection. For example, if a new database is being created, and if it contains Internal Use Only and Confidential information, then the entire database must be classified as Confidential. Other examples of such collections include an internally-generated competitive intelligence report, management decision background reports, and access-controlled intranet pages. At the time that it is being compiled, every worker creating a new collection of this nature must notify the involved information Owner about the creation of their new collection.

Storage Media—If information recorded on computer storage media with a higher sensitivity classification is moved to media with a lower sensitivity classification, then the media with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity classification. If information with several different data classification levels is resident on a single computer, then the system controls must reflect the requirements associated with most restrictive data classification level. In general, because it increases handling costs and operational complexity, commingling information with different sensitivity classifications is discouraged.

Labels For Externally-Supplied Information—With the exception of general business correspondence and copyrighted software, all externally-provided information that is not clearly in the public domain must receive a GradLeaders USA, LLC. data classification system label. The GradLeaders USA, LLC. worker who receives this information is responsible for assigning an appropriate classification on behalf of the external party. When assigning a GradLeaders USA, LLC. classification label, this staff member must preserve copyright notices, author credits, guidelines for interpretation, and information about restricted dissemination.

Labeling Hardcopy—All printed, handwritten, or other paper manifestations of sensitive information must have a clearly-evident sensitivity label on the upper right hand corner of each page. If bound, all paper manifestations of sensitive information must have an appropriate sensitivity label on the front cover, the title page, and the rear cover. The cover sheet for faxes containing sensitive information must contain the appropriate classification label.

Labeling Computer Storage Media—All CD-ROMs, floppy disks, and other computer storage media containing sensitive information must be externally labeled with the appropriate sensitivity classification. Unless it would adversely affect the operation of an application program, computer files containing sensitive information must also clearly indicate the relevant classification label in the first two data lines.

Other Displays—If information is sensitive, all instances in which it is displayed on a screen or otherwise presented to a computer user must involve an indication of the information's sensitivity classification. Teleconferences and telephone conference calls where sensitive information will be discussed must be preceded by a statement about the sensitivity of the information involved. Teleconferences and telephone calls where sensitive information is discussed must be preceded by a determination that all parties to the discussion are authorized to receive the sensitive information. Persons other than those specifically invited must not attend meetings where sensitive information will be discussed.

Additional Public Information Labels—Unless it is unquestionably already public information, all GradLeaders USA, LLC. information with a Public label must also be labeled “Approved For Public Release” along with the date when the Owner declared the information Public.

Third-Party Interactions

Third Parties And The Need To Know—Unless it has been specifically designated as Public, all GradLeaders USA, LLC. internal information must be protected from disclosure to third parties. Third parties may be given access to GradLeaders USA, LLC. internal information only when a demonstrable need to know exists, and when such a disclosure has been expressly authorized by the relevant GradLeaders USA, LLC. information Owner. Contractors, consultants, temporaries, volunteers and every other type of individual or entity that is not a GradLeaders USA, LLC. employee, is by definition a third party for purposes of this policy.

Disclosures To Third Parties And Non-Disclosure Agreements—The disclosure of sensitive information to consultants, contractors, temporaries, or any other third parties must be preceded by the receipt of a signed GradLeaders USA, LLC. non-disclosure agreement.

Disclosures From Third Parties And Non-Disclosure Agreements—Workers must not sign non-disclosure agreements provided by third parties without the authorization of GradLeaders USA, LLC. legal counsel designated to handle intellectual property matters. These forms may contain terms and conditions that unduly restrict the future business directions of GradLeaders USA, LLC.

Third-Party Requests For GradLeaders USA, LLC. Information—Unless a worker has been authorized by the information Owner to make public disclosures, all requests for information about GradLeaders USA, LLC. and its business must be referred to the information Owner. Such requests include questionnaires, surveys, and newspaper interviews. This policy does not apply to sales and marketing information about GradLeaders USA, LLC. products and services, nor does it pertain to customer support calls.

Prior Review—Every speech, presentation, technical paper, book, or other communication to be delivered to the public must have been approved for release by the involved employee's immediate manager. This policy applies if the employee will represent GradLeaders USA, LLC. or discuss GradLeaders USA, LLC. affairs, or if the communication is based on information obtained in the course of performing GradLeaders USA, LLC. job duties.

Owner Notification—If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information Owner and the manager of the Information Security department must be notified immediately.

Declassification and Downgrading

Dates For Reclassification—If known, the date that Secret or Confidential information will no longer be sensitive or declassified must be indicated on all GradLeaders USA, LLC. sensitive information. This will assist those in possession of the information with its proper handling, even if these people have not been in recent communication with the information's Owner. Those workers in possession of sensitive information that was slated to be declassified on a date that has come and gone, but is not known definitively to have been declassified, must check with the information Owner before they disclose the information to any third parties.

Classification Extensions—The designated information Owner may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at its current classification level. To achieve this, the Owner must change the declassification or downgrading date appearing on the original document, notify all known recipients and Custodians, initiate a cost-effective search for additional recipients, and notify the GradLeaders USA, LLC. archives Custodian. Owners must not to specify a date for declassification or downgrading unless they are relatively sure that the date will not be changed.

Notifications—The designated information Owner may, at any time, declassify or downgrade the classification of information entrusted to his or her care. To achieve this, the Owner must change the classification label appearing on the original document, notify all known recipients and Custodians, and notify the GradLeaders USA, LLC. archives Custodian.

Schedule For Review—To determine whether sensitive information may be declassified or downgraded, at least once annually, information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical. Owners must follow the guidelines for declassification and downgrading as specified in the information ownership policy [a link to that policy could be placed here].

No Unauthorized Downgrading—Workers must not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of a declassification or downgrading process approved by the Owner.

Destruction and Disposal

Destruction And Disposal—All GradLeaders USA, LLC. information must be destroyed or disposed of when no longer needed for business purposes. To support this policy, information Owners must review the continued value and usefulness of information on a periodic basis. Owners also must review the data retention schedule to determine the minimum legal periods that information must be retained.

Destruction And Locked Boxes—All sensitive information no longer being used or no longer needed must be placed in designated locked boxes until such time as authorized GradLeaders USA, LLC. personnel or a bonded destruction service picks it up. If no locked disposal boxes are in the immediate vicinity, sensitive information in hardcopy form must be either shredded or incinerated, while sensitive information in all other forms must be delivered to the Information Security department for secure destruction. The shredders used for this purpose must create confetti or other similar small particles. Strip-cut shredders must not be used for this purpose. Erasing or reformatting magnetic media such as floppy disks is not an acceptable data destruction method. The use of overwriting programs approved by the Information Security department is permissible as a way to destroy sensitive information on magnetic storage media such as floppy disks. Only after these programs have been used can storage media containing sensitive information be reused, trashed, recycled, or donated to charity.

Destruction Approval—Workers must not destroy or dispose of potentially important GradLeaders USA, LLC. records or information without specific advance management approval. Unauthorized destruction or disposal of GradLeaders USA, LLC. records or information will subject the worker to disciplinary action including termination and prosecution. Records and information must be retained if they are likely to be needed in the future, regulation or statute requires their retention, or they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts. Any questions about data destruction must be referred to the information Owner or the Owner's delegate.

Permissible Destruction—Workers may destroy GradLeaders USA, LLC. records when approval has been granted by verbal instructions from the Owner or the Owner's delegate, or Information Security department memo detailing the type of records that may be destroyed and when. Destruction is defined as any action that prevents the recovery of information from the storage medium on which it is recorded.

Photocopies—All waste copies of Secret information that are generated in the course of copying, printing, or other sensitive information handling must be destroyed according to the instructions found in this policy. If a copy machine jams or malfunctions when workers are making copies of Secret information, the involved workers must not leave the machine until all copies of the information are removed from the machine or destroyed beyond recognition.

Equipment Disposal Or Servicing—Before computer or communications equipment is sent to a vendor for trade, servicing, or disposal, all GradLeaders USA, LLC. sensitive information must be destroyed or concealed according to methods approved by the Information Security department. Internal hard drives and other computer storage media may not be donated to charity, disposed of in the trash, or otherwise recycled unless they have been subjected to overwriting processes approved by the Information Security department.

Special Considerations for Secret Information

Storage On Personal Computers—If Secret information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must support and continuously run an access control package approved by the Information Security department. When these users are not currently accessing or otherwise actively using the Secret information on such a machine, they must not leave the machine without logging off, invoking a screen saver, or otherwise restricting access to the Secret information.

Numbering Document Copies—All copies of Secret documents must be individually numbered with a sequence number to ensure that the persons responsible for the documents and the location of the documents can both be readily tracked. Hardcopy manifestations of Secret information must include the words "Do Not Copy Without Explicit Permission From The Information Owner."

Secret Information Logs—When Secret information is involved, the Owner or delegate of the Owner must keep a log reflecting the number of copies made, the location of copies, the names of recipients, the addresses of recipients, and any persons viewing the copies. This log must be maintained as long as such information retains a Secret sensitivity classification. This log also must be classified as Secret. All production application systems that handle Secret GradLeaders USA, LLC. information must generate logs that show every addition, modification, and deletion to such Secret information.

Removal From Offices—Secret GradLeaders USA, LLC. information must not leave GradLeaders USA, LLC. offices unless the approval of the Information Security manager has been obtained.

Couriers—Secret information in hardcopy form must be sent by trusted courier or registered mail. Other methods such as regular mail are prohibited. All deliveries of Secret information must be conducted such that the intended recipient personally acknowledges that the information has been received. Delivery of Secret information to intermediaries such as receptionists is prohibited.

Transportation With Computers—Workers in the possession of portable, laptop, notebook, handheld, personal digital assistant, and other transportable computers containing Secret GradLeaders USA, LLC. information must not leave these computers unattended at any time unless the Secret information has been encrypted. If Secret data is to be transported in computer-readable storage media, it must be in encrypted form.

Viewing In Public—Workers must avoid traveling on public transportation when in the possession of Secret information. Secret information must not be read, discussed, or otherwise exposed on airplanes, or in restaurants, elevators, restrooms, or other public places. GradLeaders USA, LLC. workers must not take Secret GradLeaders USA, LLC. information into another country unless permission has been obtained from the Information Security manager.

Storage—Computerized Secret information must be encrypted when not in active use. All systems used for the processing of Secret information must be powered down immediately after processing is completed, or have these temporary storage locations overwritten with programs approved by the Information Security department.

Transmission Over Networks—If GradLeaders USA, LLC. Secret data is to be transmitted over any communication network, it must be sent only in encrypted form. Such networks include internal electronic mail systems, the Internet, and dial-up lines. All such transmissions must use a virtual public network or similar software as approved by the Information Security department.

Transfer To Another Computer—Before any Secret information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

Fax Transmission—Secret information must not be sent to an unattended fax machine unless the destination machine is in a locked room for which only people authorized to receive the information possess the keys. Transmission to a fax server

that uses passwords to control access to received faxes is a permissible exception to this policy. All fax transmissions containing Secret data must also employ an encrypted link.

Speaker Phones—Secret information must not be discussed on speakerphones unless all participating parties acknowledge that no unauthorized persons are in close proximity such that they might overhear the conversation. Workers must refrain from leaving messages containing Secret information on answering machines or voice mail systems.

Telephone Conversations—Workers must take steps to avoid discussing sensitive information when on the telephone. If discussion of such information is absolutely required, workers must use guarded terms and refrain from mentioning sensitive details beyond those needed to get the job done.

External Party Disclosure

Determining If Disclosure Is Appropriate

Duty to Take Special Care—To the extent required to perform their job duties, workers are given access to GradLeaders USA, LLC. sensitive internal information. Proper protection of this information is essential if the interests of not only GradLeaders USA, LLC., but also customers and business partners, are to be preserved. These interests include maintenance of competitive advantage, trade secret protection, and preservation of personal privacy. As indicated in the non-disclosure agreement signed by all workers, special care must be taken to prevent disclosure of sensitive internal information to unauthorized third parties.

Sources of Additional Information—While this policy describes the considerations that workers should bear in mind before, during, and after disclosure to third parties, it cannot specifically address every possible situation. Questions about the disclosure of specific information must be directed to the relevant information Owner. Additionally, workers are expected to extend these policies to fit the specific circumstances they face, to use their professional judgment, and ask the Information Security department for guidance in those instances where the appropriate handling of sensitive information is unclear.

Two Types of Information—For the purpose of this policy, there are basically two types of information. The first type of information has been approved for release to a specific group such as customers, an organization such as a regulatory agency, or an individual such as a contractor. Information that has been specifically designated as Public also falls into this first category. If the party requesting information falls within the limits of the approved group of recipients, or if the Public label has been applied, then no Owner approval is required. The second type of information has not yet been approved for release to a specific group, organization, or individual. This policy discusses the specific requirements for dealing with the second category. Additional guidance may be found in the Information Classification Policy.

Third Parties and The Need To Know—Unless it has specifically been designated as Public, all GradLeaders USA, LLC. internal information must be protected from unauthorized disclosure to third parties. Third parties may be given access to GradLeaders USA, LLC. internal information only when a demonstrable need to know exists, and when such a disclosure has been expressly authorized by the relevant GradLeaders USA, LLC. information Owner.

Non-Disclosure Agreements—The disclosure of sensitive information to consultants, contractors, temporaries, volunteers, outsourcing organization staff, and other third parties must be preceded by the receipt of a signed non-disclosure agreement (NDA). When an NDA pertains to an organization, to be valid, an officer of the recipient organization must sign the NDA. Workers must not sign NDAs provided by third parties without the advance authorization of GradLeaders USA, LLC. legal counsel designated to handle intellectual property matters.

Disclosing Information Belonging to Third Parties—GradLeaders USA, LLC. workers must not disclose third-party information to other third parties unless the third party providing the information or the legal Owner of the information

has provided advance approval of the disclosure. Even when this disclosure has been approved in advance, the receiving party must sign a non-disclosure agreement.

Third-Party Requests for GradLeaders USA, LLC. Information—Unless a worker has been authorized by the information Owner to make disclosures, all requests for information about GradLeaders USA, LLC. and its business must be referred to the Public Relations department [insert an intranet link to that department's page]. Such requests include questionnaires, surveys, and newspaper interviews. This policy does not apply to sales and marketing information about GradLeaders USA, LLC. products and services, nor does it pertain to customer requests for information that has been approved for release to customers.

Prior Review—Every speech, presentation, technical paper, book, or other communication to be delivered to the public must be approved for release by the involved employee's immediate manager. This policy applies if the employee will represent GradLeaders USA, LLC. or discuss GradLeaders USA, LLC. affairs, or if the communication is based on information obtained in the course of performing GradLeaders USA, LLC. duties. If new products, research results, corporate strategies, customer information, or marketing approaches are to be divulged, approval of the director of Research and Development and the director of the Legal department must be obtained.

Releasing Information About Internal Events—Specific information about GradLeaders USA, LLC. internal events, including new products and services, staff promotions, reorganizations, and information system problems, must not be released to third parties, including members of the news media, without specific authorization from the senior management.

Discussions In Public Forums—Care must be taken to properly structure comments and questions posted to electronic bulletin boards, mailing lists, online news groups, and related forums on public networks like the Internet. Care must be taken when wording requests for proposals and help wanted advertisements so that strategic directions, new products, and other sensitive information are not indirectly divulged. If a worker is part of a project team developing an unannounced new product or service, a research and development effort, or related confidential GradLeaders USA, LLC. matters, all related postings must be cleared with one's manager prior to being posted to any public network. Workers must be careful not to reveal specifics about GradLeaders USA, LLC. internal systems through public postings.

Preparing Information for Disclosure

Using The Best Information—Authorized disclosures of GradLeaders USA, LLC. internal information must be performed with the most current, accurate, timely, and relevant information available. The worker disclosing the information must be aware of and extract the information from the system of record, or the definitive master copy of such information within GradLeaders USA, LLC.

Updates To Previously Disclosed Information—Owners must have correct information that has been made public, or that has been disclosed to certain third parties, if subsequent events have made this information misleading or materially incorrect. Timely and prompt correction of the previously disclosed information is especially important in those instances where the public or a third party is likely to rely on the information in its decision-making processes. This requirement does not apply if the disclosure took place a year or more in the past, and the information is unlikely to be in use.

Designated Source For Public Disclosures—Information generated by GradLeaders USA, LLC. and released to the public must be accompanied by the name of a designated staff member acting as the single recognized official source and point of contact. All updates and corrections to this information that are released to the public must flow through this official source.

Resolving Problems with Disclosure Processes

Unassigned Owner—If the GradLeaders USA, LLC. internal information being considered for disclosure to a third party does not have a designated Owner, then the disclosure decision must be made by the GradLeaders USA, LLC. Information Security manager. Workers also can ask the designated information Custodian to identify the Owner.

Unmarked Information—If the information being considered for disclosure to third parties is not marked with an appropriate information classification, workers must assume that the information is GradLeaders USA, LLC. Internal Use Only information, and not approved for public release. Information marked Public does not require Owner approval prior to release to third parties.

Marking Preservation—The worker disclosing GradLeaders USA, LLC. internal information to third parties must preserve markings indicating author, date, version number, usage restrictions, and other details that might be useful in determining the approved usage, currency, accuracy, and relevance of the information. An exception may be made, with Owner approval, in those cases where such markings would reveal GradLeaders USA, LLC. information that should not be disclosed to the third party.

Disclaimers—It is the information Owner's responsibility to ensure that when controversial, frequently changing, highly uncertain, or potentially-damaging information is released to third parties that it contain the appropriate legal disclaimers. Such disclaimers, generally provided by the GradLeaders USA, LLC. Legal counsel, include words that limit GradLeaders USA, LLC. liability, define the information's intended uses, and inform recipients of potential problems associated with the information.

Recovery or Destruction—All copies of Secret information provided to third parties must be returned to the worker within GradLeaders USA, LLC. who provided it. All such copies must be destroyed. Such recovery or destruction must occur within a month of the time when the information ceases to be useful for the intended purposes. The GradLeaders USA, LLC. worker who provided the information is responsible for recovering the information. This GradLeaders USA, LLC. worker must note the recovery or destruction of the information in his or her records reflecting disclosures.

Reporting Improper Disclosures—If sensitive information has been inappropriately disclosed, or is believed to have been inappropriately disclosed, the circumstances must be reported immediately to the relevant information Owner. If an Owner has not been assigned for the information, Information Security department must be informed immediately. It is the Owner's responsibility to determine whether the disclosure or suspected disclosure must be reported to third parties such as government banking regulators, criminal justice system personnel, customers, and others. If no Owner has been assigned, this decision is the Information Security department's responsibility.

Network Security

Introduction

Purpose - The purpose of this policy is to establish management direction, procedural requirements, and technical guidance to ensure the appropriate protection of GradLeaders USA, LLC. information handled by computer networks.

Scope - This policy applies to all employees, contractors, consultants, temporaries, volunteers, and other workers at GradLeaders USA, LLC., including those workers affiliated with third parties who access GradLeaders USA, LLC. computer networks. Throughout this policy, the word “worker” will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by or administered by GradLeaders USA, LLC.

General Policy - All information traveling over GradLeaders USA, LLC. computer networks that has not been specifically identified as the property of other parties will be treated as though it is a GradLeaders USA, LLC. corporate asset. It is the policy of GradLeaders USA, LLC. to prohibit unauthorized access, disclosure, duplication, modification, diversion,

destruction, loss, misuse, or theft of this information. In addition, it is the policy of GradLeaders USA, LLC. to protect information belonging to third parties that have been entrusted to GradLeaders USA, LLC. in a manner consistent with its sensitivity and in accordance with all applicable agreements.

Responsibilities

An information security management committee will be composed of middle-level managers or their delegates from each GradLeaders USA, LLC. division, and the director of Information Technology, the director of Security, and the chief information office. At quarterly and ad hoc meetings, this committee will periodically review the status of GradLeaders USA, LLC. computer and network security, review and monitor remedial work related to computer and network security incidents, authorize and later judge the results of major projects dealing with computer and network security, approve new or modified information security policies, standards, guidelines, and procedures, and perform other high-level information security management activities.

The Information Security manager is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems security policies, standards, guidelines, and procedures. This manager also is responsible for activities related to this policy. While responsibility for information systems security on a day-to-day basis is every worker's duty, specific guidance, direction, and authority for information systems security is centralized for all of GradLeaders USA, LLC. and its subsidiaries in the Information Security department. This department will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

The Physical Security manager is responsible for conducting investigations into any alleged computer or network security compromises, incidents, or problems. All compromises or potential compromises must be immediately reported to the Physical Security manager.

System administrators are responsible for acting as local information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. They also are responsible for reporting all suspicious computer and network-security-related activities to the Physical Security manager. System administrators also implement the requirements of this and other information systems security policies, standards, guidelines, and procedures

Departmental managers are responsible for ensuring that appropriate computer and communication system security measures are observed in their areas. Besides allocating sufficient resources and staff time to meet the requirements of these policies, departmental managers are responsible for ensuring that all users are aware of GradLeaders USA, LLC. policies related to computer and communication system security.

Users are responsible for complying with this and all other GradLeaders USA, LLC. policies defining computer and network security measures. Users also are responsible for bringing all known information security vulnerabilities and violations that they notice to the attention of the Physical Security manager.

Physical Security

All doors leading to outside of GradLeaders USA, LLC offices must remain locked at all times.

Access to systems development staff offices, telephone wiring closets, computer machine rooms, network switching rooms, and other work areas containing Confidential or Secret information must be physically restricted. Management responsible for the staff working in these areas must consult the Information Security department to determine the appropriate access control method.

Workers must not attempt to enter restricted areas in GradLeaders USA, LLC buildings for which they have not received access authorization.

When a worker terminates a working relationship with GradLeaders USA, LLC, all physical security access codes known by or available to the worker must be deactivated or changed.

Confidential or Secret information must not be downloaded to remote locations, such as sales offices, unless proper physical security and encryption facilities are installed and faithfully observed.

Visitors to GradLeaders USA, LLC offices including, but not limited to, customers, former employees, worker family members, equipment repair contractors, package delivery company staff, and police officers, must be escorted at all times by an authorized worker.

Whenever a worker notices an unescorted visitor inside GradLeaders USA, LLC restricted areas, the visitor must be questioned about the purpose for being in restricted areas, then be accompanied to a reception desk, a guard station, or the person they came to see.

Every third party repair person or maintenance person who shows up at GradLeaders USA, LLC facilities without being called by an employee must be denied access to the facilities. All such incidents must be promptly reported to the Information Security Department. Those that have been called by an employee must have their requested presence confirmed by a guard or receptionist before they are given access to the facilities.

System Access Control

End-User Passwords - Users must choose fixed passwords that are difficult to guess. This means that passwords must not be related to a user's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used. Where this type of systems software is available, users must be prevented from selecting easily-guessed passwords.

Users can choose easily-remembered passwords that are difficult for unauthorized parties to guess if they:

- String together several words into a pass phrase.
- Shift a word up, down, left, or right one row on the keyboard.
- Bump characters in a word a certain number of letters up or down the alphabet.
- Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word.
- Combine punctuation or numbers with a regular word.
- Create acronyms from words in a song, a poem, or another known sequence of words.
- Deliberately misspell a word.
- Combine a number of personal facts like birth dates and favorite colors.

Users must not construct passwords that are identical or similar to passwords they have previously employed. Where systems software facilities are available, users must be prevented from reusing previous passwords.

Users must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must not employ passwords like “X34JAN” in January and “X34FEB” in February.

Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in data communications software, in web browsers, on hard drives, or in other locations where unauthorized persons might discover them.

Passwords must not be written down and left in a place where unauthorized persons might discover them. Aside from initial password assignment and password-reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password must be changed immediately.

Passwords must never be shared or revealed to anyone else besides the authorized user. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms. This policy does not prevent the use of default passwords, typically used for new user ID assignment or password reset situations, which are then immediately changed when the user next logs onto the involved system. All passwords must be immediately changed if they are suspected of being disclosed or known to have been disclosed to anyone other than the authorized user.

Password System Setup - All computers permanently or intermittently connected to GradLeaders USA, LLC. networks must have password access controls. If the computers contain Confidential or Secret information, an extended user authentication system approved by the Information Security department must be used. At the very least, multi-user systems must employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual's need to know. Network-connected, single-user systems must employ hardware or software controls approved by Information Security that prevent unauthorized access including a screen blanker triggered by a certain period of no keyboard activity.

Unless an extended user authentication system is involved, computer and communication system access control must be achieved through fixed passwords that are unique to each individual user. Access control to files, applications, databases, computers, networks, and other system resources through shared passwords or group passwords is prohibited.

Wherever systems software permits, the display and printing of fixed passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

Wherever systems software permits, the initial fixed passwords issued to a new user by a security administrator must be valid only for the user's first online session. At that time, the user must be required to choose another password. This same process applies to the resetting of passwords in the event that a user forgets a password.

All vendor-supplied default fixed passwords must be changed before any computer or communications system is used for production GradLeaders USA, LLC. business. This policy applies to passwords associated with end-user user IDs and passwords associated with privileged user IDs.

Where systems software permits, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three unsuccessful attempts to enter a password, the involved user ID must be suspended until reset by a system administrator or temporarily disabled for no less than three minutes. If dial-up connections are involved, the session must be disconnected. If DSL, ISDN, cable modem, or other constant connections are employed, a time-out period must be initiated.

Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the involved system administrator must immediately change all involved privileged user passwords and require every end-user password on the involved system to be changed at the time of the next log on. If systems software does not provide the latter capability, a broadcast message must be sent to all users telling them to change their passwords immediately.

Logon and Logoff Process - All users must be positively identified prior to being able to use any GradLeaders USA, LLC. multi-user computer or communications system resources. Positive identification for internal GradLeaders USA, LLC. networks involves a user ID and fixed password, both of which are unique to an individual user, or an extended user authentication system.

The logon process for network-connected GradLeaders USA, LLC. computer systems must simply ask the user to log on, providing prompts as needed. Specific information about the organization managing the computer, the computer operating system, the network configuration, or other internal matters must not be provided until a user has successfully provided both a valid user ID and a valid password.

If there has been no activity on a computer terminal, workstation, or personal computer for a certain period of time, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. The recommended period of time is 15 minutes. An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room badge readers, or similar technology.

With the exception of electronic bulletin boards or other systems where all regular users are anonymous, users are prohibited from logging into any GradLeaders USA, LLC. system or network anonymously, for example, by using guest user IDs. If users employ systems facilities that permit them to change the active user ID to gain certain privileges, they must have initially logged on employing a user ID that clearly indicates their identity.

System Privileges

Limiting System Access - The computer and communications system privileges of all users, systems, and independently-operating programs such as agents, must be restricted based on the need to know. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

Default user file permissions must not automatically permit anyone on the system to read, write, execute or delete a file. Although users may reset permissions on a file-by-file basis, such permissive default file permissions are prohibited. Default file permissions granted to limited groups of people who have a genuine need to know are permitted.

Users with personal computers are responsible for administering a screen saver program securing access to their machine's hard disk drive, and setting passwords for all applications and systems software that provide the capability.

GradLeaders USA, LLC. computer and communications systems must restrict access to the computers that users can reach over GradLeaders USA, LLC. networks. These restrictions can be implemented through routers, gateways, firewalls, and other network components. These restrictions must be used to, for example, control the ability of a user to log on to a certain computer then move from that computer to another.

Process for Granting System Privileges - Requests for new user IDs and changed privileges must be in writing and approved by the user's manager before the Information Security department fulfills these requests.

Individuals who are not GradLeaders USA, LLC. employees must not be granted a user ID or be given privileges to use GradLeaders USA, LLC. computers or networks unless the written approval of a department head has been obtained.

Privileges granted to users who are not GradLeaders USA, LLC. employees must be granted for periods of 90 days or less. As needed, users who are not GradLeaders USA, LLC. employees must have their privileges reauthorized by the sponsoring department head every 90 days.

Special privileges, such as the default ability to write to the files of other users, must be restricted to those responsible for systems administration or systems security. An exception to this policy can be made if a department head has approved the exception in writing. Configuration changes, operating system changes, and related activities that require system privileges must be performed by system administrators, not end users.

Third-party vendors must not be given Internet or dial-up privileges to GradLeaders USA, LLC. computers or networks unless the system administrator determines that they have a legitimate business need. These privileges must be enabled only for the time period required to accomplish the approved tasks, such as remote maintenance. If a perpetual or long-term connection is required, then the connection must be established by approved extended user authentication methods.

All users wishing to use GradLeaders USA, LLC. internal networks, or multi-user systems that are connected to GradLeaders USA, LLC. internal networks, must sign a compliance statement prior to being issued a user ID. If a certain user already has a user ID, a signature must be obtained prior to receiving a renewed user ID. The latter process must be performed periodically.

Process for Revoking System Access - All user IDs must have the associated privileges revoked after a certain period of inactivity not exceeding 90 days.

If a computer or communication system access control subsystem is not functioning properly, it must default to denial of privileges to users. If access control subsystems are malfunctioning, the systems must remain unavailable until such time as the problem has been rectified.

Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Information Security manager. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of GradLeaders USA, LLC. policy. Customer requests that GradLeaders USA, LLC. security mechanisms be compromised must not be satisfied unless the Information Security manager approves in advance or GradLeaders USA, LLC. is compelled to comply by law. Short-cuts bypassing systems security measures, pranks, and practical jokes involving the compromise of systems security measures are absolutely prohibited.

The privileges granted to users must be reevaluated by management every six months. In response to feedback from this review, system administrators must promptly revoke all privileges no longer needed by users.

Management must report all significant changes in worker duties or employment status promptly to the system administrators responsible for user IDs associated with the involved persons. For all terminations, the Human Resources department also must issue a notice of status change to the system administrator who might be responsible for a system on which the involved worker might have a user ID.

Establishment of Access Paths - Changes to GradLeaders USA, LLC. internal networks include loading new software, changing network addresses, reconfiguring routers, and adding dial-up lines. With the exception of emergency situations, all changes to GradLeaders USA, LLC. computer networks must be approved in advance by Information Technology except as delegated by Information Technology. Emergency changes to networks must be made by persons who are authorized by Information Technology. This process prevents unexpected changes from leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to workers, but also to vendor personnel.

Workers must not establish electronic bulletin boards, local area networks, FTP servers, web servers, modem connections to existing local area networks, or other multi-user systems for communicating information without the specific approval of the Information Security manager. New types of real-time connections between two or more in-house computer systems must not be established unless such approval is obtained.

Participation in external networks as a provider of services that external parties rely on is prohibited unless GradLeaders USA, LLC. legal counsel has identified the legal risks involved and the director of Information Technology has expressly accepted these and other risks associated with the proposal.

All GradLeaders USA, LLC. computers that connect to an internal or external network must employ password-based access controls or an extended user authentication system. Multi-user computers must employ software that restricts access to the files of each user, logs the activities of each user, and has special privileges granted to a system administrator. Single-user systems must employ access control software approved by the Information Security department that includes boot control and an automatic screen blanker that is invoked after a certain period of no input activity. Portable computers and home computers that contain GradLeaders USA, LLC. information are also covered by this policy, as are network devices such as firewalls, gateways, routers, and bridges.

All inter-processor commands from non-GradLeaders USA, LLC. locations are prohibited unless a user or process has properly logged on. Examples of such commands include remotely-initiated requests for a list of users currently logged on and a remote procedure call.

Users initiating sessions through dial-up lines connected to GradLeaders USA, LLC. internal networks or multi-user computer systems must pass through an additional access control point or firewall before users employing these lines can reach a logon banner. Unless approved in advance by the director of Information Security, dial-up connections that do not

go through approved firewalls in order to reach GradLeaders USA, LLC. internal-network connected systems are prohibited. This policy applies to Internet inbound calls and electronic data interchange.

Remote maintenance ports for GradLeaders USA, LLC. computer and communication systems must be disabled until the time they are needed by the vendor. These ports must be disabled immediately after use. Dial-up connections can be established with vendors through outbound calls initiated by GradLeaders USA, LLC. workers. No firewall access control is needed for either type of connection.

Portable phones using radio technology and cellular phones must not be used for data transmissions containing GradLeaders USA, LLC. confidential or secret information unless the connection is encrypted. Other broadcast networking technologies, such radio-based local area networks, must not be used for these types of GradLeaders USA, LLC. information unless the link is encrypted. Such links may be used for electronic mail as long as users understand that confidential or secret information must not be transmitted using this technology.

Computer Viruses, Worms, And Trojan Horses

Users must keep approved and current virus-screening software enabled on their computers. This software must be used to scan all software coming from third parties or other GradLeaders USA, LLC. departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

Users are responsible for eradicating viruses from all personal computer systems under their control whenever viruses have been detected using software installed by GradLeaders USA, LLC. staff. As soon as a virus is detected, the involved user must immediately contact the Information Security department to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged.

All personal computer software must be copied prior to its initial usage, and such copies must be stored in a safe place. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems. These master copies also must be stored in a secure location.

GradLeaders USA, LLC. computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the Information Security manager.

Data and Program Backup

Personal computer users are responsible for backing up the information on their machines. For multi-user computer and communication systems, the Information Technology department is responsible for making periodic backups. If requested, the Information Technology department will install or provide technical assistance for the installation of backup hardware or software.

All sensitive information such as Confidential or Secret, valuable, or critical, resident on GradLeaders USA, LLC. computer systems and networks must be periodically backed up. User department managers must define which information and which machines are to be backed up, the frequency of backup, and the method of backup based on the following guidelines:

- If the system supports more than one individual and contains data that is critical to day-to-day operations within GradLeaders, LLC., then a backup is required daily.

- If the system is used to support job-related functions and contains key data critical to the day-to-day operations of that job, then a backup is required weekly.
- If the system is primarily used as a personal productivity tool and contains no data that would be classified as job or departmental in nature, then a backup is at the discretion of the individual user.

Nothing in the time frames for periodic backup mentioned immediately above restricts the generation of more frequent backups, as will occasionally be required for operational and business reasons.

GradLeaders USA, LLC. requires the use of at least three sets of backup storage media to be used in rotation. For multi-user machines, whenever systems software permits, backups must be performed without end-user involvement, over an internal network and during the off hours.

Storage of backup media is the responsibility of the multi-user machine system administrator involved in the backup process. Media must be stored in fireproof safes, at a separate location at least several city blocks away from the system being backed up.

All GradLeaders USA, LLC. Confidential or Secret information stored on backup computer media must be encrypted using approved encrypting methods.

Encryption

When GradLeaders USA, LLC. Confidential or Secret information is transmitted over any communication network, it must be sent in encrypted form. Whenever GradLeaders USA, LLC. source code, or source code that has been entrusted to GradLeaders USA, LLC. by a business partner, is to be sent over a network, it too must be in encrypted form. Specific definitions of the words “Confidential” and “Secret” can be found in the Data Classification Policy.

Whenever Confidential or Secret information is not being actively used, it must be stored in encrypted form. This means that when this information is stored or transported in computer-readable storage media, it must be in encrypted form.

Encryption of information in storage or in transit must be achieved through commercially-available products approved by the Information Security department.

Whenever encryption is used, workers must not delete the sole readable version of the information unless they have demonstrated that the decryption process is able to reestablish a readable version of the information.

Encryption keys used for GradLeaders USA, LLC. information are always classified as Confidential or Secret information. Access to such keys must be limited only to those who have a need to know. Unless the approval of the Information Security manager is obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or other third parties. Encryption keys always must be encrypted when sent over a network.

Whenever such facilities are commercially available, GradLeaders USA, LLC. must employ automated rather than manual encryption key management processes for the protection of information on GradLeaders USA, LLC. networks.

Logs And Other Systems Security Tools

Every multi-user computer or communications system must include sufficient automated tools to assist the system administrator in verifying a system's security status. These tools must include mechanisms for the recording, detection, and correction of commonly-encountered security problems.

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical GradLeaders USA, LLC. information must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passwords, attempts to use

privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges, and changes to logging system configurations.

Logs containing computer or communications system security relevant events must be retained for at least 90 days. During this period, logs must be secured such that they cannot be modified, and such that only authorized persons can read them.

Certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information must be securely stored offline until such time as it is determined that GradLeaders USA, LLC. will not pursue legal action or otherwise use the information. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files.

Records reflecting security relevant events must be periodically reviewed in a timely manner by computer operations staff, information security staff, or systems administration staff.

Users must be informed of the specific acts that constitute computer and network security violations. Users must also be informed that such violations will be logged.

Although system administrators are not required to promptly load the most recent version of operating systems, they are required to promptly apply all security patches to the operating system that have been released by knowledgeable and trusted user groups, well-known systems security authorities, or the operating system vendor. Only those systems security tools supplied by these sources or by commercial software organizations may be used on GradLeaders USA, LLC. computers and networks.

Remote Printing

Printers must not be left unattended if Confidential or Secret information is being printed or soon will be printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

Production Data Center

Special Considerations - The purpose of this policy is to indentify special considerations for security necessary at GradLeaders USA, LLC production facilities and data center. Unless otherwise noted in this policy all Network Security policies remain applicable.

Limiting System Access - Only information owners and custodians determined to have a “need to know” will be granted privileges to access GradLeaders USA, LLC production computer equipment. This may include support personnel and other members of the technology team that require access to perform their duties. Determination for such workers will be made exclusively by the Information Security Manager.

Process for Granting System Privileges - Requests for new user IDs and changed privileges must be in writing and approved by the user's manager before the Information Security department fulfills these requests. The manager must demonstrate a genuine “need to know” before requests will be granted.

Data Backups - The Information Technology department is solely responsible for making periodic backups of production network files and databases.

- GradLeaders USA, LLC. requires the use of at least four full backup sets of storage media to be used in a weekly rotation. Differential backups of all production network storage will be made on a daily basis and stored on separate media.
- Off-Site storage at least three of the four full backup sets must be maintained. Off-Site storage of this media is handled by BlueBridge Networks (see Appendix for details).
- All production network backups must be encrypted using no less that 256-bit encryption technology.

SQL Databases – All SQL Databases in the production data center will grant access based on the network integrated security. Use of SQL stand alone security should be limited to special circumstances and approved by the Information Security Manager.

Direct access to SQL Databases must be limited to information custodians and approved by the Information Security Manager. Access should be limited to "read only" except when designated by the Information Security Manager.

All data stored in SQL databases in the production datacenter should be considered "secret" for purposes of data classification.

All SQL Database servers must employ full point in time backups with transaction logs. Transaction logs must be backed up every two hours and full database backups must occur nightly. All SQL transaction log and database backups must be stored in at least two physical locations on the network and at least one off-site storage location.

Physical Security – See Appendix A – Expedient

Privacy

Unless contractual agreements dictate otherwise, messages sent over GradLeaders USA, LLC. computer and communications systems are the property of GradLeaders USA, LLC. Management reserves the right to examine all data stored in or transmitted by these systems. Because GradLeaders USA, LLC. computer and communication systems must be used for business purposes only, workers must have no expectation of privacy associated with the information they store in or send through these systems.

When providing computer-networking services, GradLeaders USA, LLC. does not provide default message protection services such as encryption. No responsibility is assumed for the disclosure of information sent over GradLeaders USA, LLC. networks, and no assurances are made about the privacy of information handled by GradLeaders USA, LLC. internal networks. In those instances where session encryption or other special controls are required, it is the user's responsibility to ensure that adequate security precautions have been taken. Nothing in this paragraph must be construed to imply that GradLeaders USA, LLC. policy does not support the controls dictated by agreements with third parties, such as organizations that have entrusted GradLeaders USA, LLC. with confidential information.

Exceptions

The Information Security manager acknowledges that under rare circumstances, certain workers will need to employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance by the Information Security manager.

Violations

GradLeaders USA, LLC. workers who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination.

Firewall Security

Policy Objective And Scope - Firewalls are an essential component of the GradLeaders USA, LLC information systems security infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. Connectivity defines which computer systems are permitted to exchange information. A service is sometimes called an application, and it refers to the way for information to flow through a firewall. Examples of services include file transfer protocol (FTP) and web browsing (HTTP).

Policy Applicability - All firewalls on GradLeaders USA, LLC networks, whether managed by employees or by third parties, must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the Information Security Manager.

Required Documentation - Prior to the deployment of every GradLeaders USA, LLC firewall, a diagram of permissible paths with a justification for each, and a description of permissible services accompanied by a justification for each, must be submitted to the Information Security Manager. Permission to enable such paths and services will be granted by the Information Security Manager only when these paths or services are necessary for important business reasons, and sufficient security measures will be consistently employed.

Default to Denial - Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by the Information Security department must be blocked by GradLeaders USA, LLC firewalls. The list of currently approved paths and services must be documented and distributed to all system administrators with a need to know by the Information Security department. An inventory of all access paths into and out of GradLeaders USA, LLC internal networks must be maintained by the Information Security department.

Connections Between Machines - Real-time connections between two or more GradLeaders USA, LLC computer systems must not be established or enabled unless the Information Security department has determined that such connections will not unduly jeopardize information security. In many cases, firewalls or similar intermediate systems must be employed. This requirement applies no matter what the technology employed, including wireless connections, microwave links, cable modems, integrated services digital network lines, and digital subscriber line connections. Any connection between an in-house GradLeaders USA, LLC production system and any external computer system, or any external computer network or service provider, must be approved in advance by the Information Security department.

Logs - All changes to firewall configuration parameters, enabled services, and permitted connectivity paths must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also must be logged. The integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least six months after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Intrusion Detection—All GradLeaders USA, LLC firewalls must include intrusion detection systems approved by the Information Security department. Each of these intrusion detection systems must be configured according to the specifications defined by the Information Security department. Among other potential problems, these intrusion detection systems must detect unauthorized modifications to firewall system files, and detect denial of service attacks in progress. Such intrusion detection systems must also immediately notify by pager the technical staff that is in a position to take corrective action. All technical staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically removed from the firewall.

External Connections—All in-bound real-time Internet connections to GradLeaders USA, LLC internal networks or multi-user computer systems must pass through a firewall before users can reach a logon banner. No GradLeaders USA, LLC computer system may be attached to the Internet unless it is protected by a firewall. The computer systems requiring firewall protection include web servers, electronic commerce servers, and mail servers.

Virtual Private Networks—To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic, with the exception of Internet mail and web site traffic, that accesses GradLeaders USA, LLC networks must be encrypted with the products approved by the Information Security department. These connections are often called virtual private networks (VPNs). The VPNs permissible on GradLeaders USA, LLC networks combine extended user authentication functionality with communications encryption functionality.

Firewall Access Mechanisms—All GradLeaders USA, LLC firewalls must have unique passwords or other access control mechanisms. The same password or access control code must not be used on more than one firewall. Whenever supported by the involved firewall vendor, those who administer GradLeaders USA, LLC firewalls must have their identity validated through extended user authentication mechanisms. .

Firewall Access Privileges—Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically-trained individuals with a business need for these same privileges. Unless permission from the Information Security Manager has been obtained, these privileges must be granted only to individuals who are full-time permanent employees of GradLeaders USA, LLC, and not to temporaries, contractors, consultants, or outsourcing personnel. All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require. Care must be taken to schedule out-of-town vacations so that at least one of these firewall administration staff members is readily available at all times.

Demilitarized Zones—All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarized zone (DMZ), a subnet that is protected from the Internet by one or more firewalls.

Disclosure Of Internal Network Information—The internal system addresses, configurations, products deployed, and related system design information for GradLeaders USA, LLC networked computer systems must be restricted such that both systems and users outside the GradLeaders USA, LLC internal network cannot access this information.

Firewall Dedicated Functionality—Firewalls must run on dedicated machines that perform no other services, such as acting as a mail server. Sensitive or critical GradLeaders USA, LLC information must never be stored on a firewall. Such information may be held in buffers as it passes through a firewall. Firewalls must have only the bare minimum of operating systems software resident and enabled on them. Where the supporting operating system permits it, all unnecessary and unused systems software must be removed from firewalls. GradLeaders USA, LLC does not permit its internal information to be resident on or processed by any firewall, server, or other computer that is shared with another organization at an outsourcing facility. Outsourcing organization-provided shared routers, hubs, modems, and other network components are permissible.

Firewall Physical Security—All GradLeaders USA, LLC firewalls must be located in locked rooms accessible only to those who perform authorized firewall management and maintenance tasks approved by the Information Technology Department management. The placement of firewalls in an open area within a general purpose data processing center is prohibited, although placement within separately locked rooms or areas, which themselves are within a general data processing center is acceptable. These rooms must be equipped with alarms and an automated log of all persons who gain entry to the room.

Personal Computers

Overview

Objectives And Scope—A large portion of GradLeaders USA, LLC. business is conducted with personal computers, including portable computers, handheld computers, personal digital assistants, and similar computers dedicated to a single user's activity. Protection of personal computers and the information handled by these systems is an essential part of doing business at GradLeaders USA, LLC. To this end, this policy provides information security instructions applicable to

all workers who use GradLeaders USA, LLC. personal computers. All personal computer users are expected to comply with this policy as a condition of continued employment. This policy applies whether personal computers are standalone or connected to a network such as a local area network or the intranet.

Business Use Only

Business Use Only—In general, GradLeaders USA, LLC. computer and communication systems are intended to be used for business purposes only. Incidental personal use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, does not preempt any business activity, and does not cause distress, legal problems, or morale problems for other workers. Permissible incidental use of a personal computer would, for example, involve responding to an electronic mail message about a luncheon, purchasing a gift online, and paying bills through the Internet. Offensive material that might cast GradLeaders USA, LLC. in a bad light, including sexist, racist, violent, or other content, is strictly forbidden from all GradLeaders USA, LLC. personal computers.

Management

Rights To Programs Developed—Without a specific written exception, all computer programs and documentation generated by, or provided by workers for the benefit of GradLeaders USA, LLC. are the property of GradLeaders USA, LLC. All other material developed by GradLeaders USA, LLC. workers using personal computers is considered the property of GradLeaders USA, LLC. This material includes patents, copyrights, and trademarks.

Browsing—Workers must not browse through GradLeaders USA, LLC. computer systems or networks. Steps taken by workers to legitimately locate information needed to perform their job are not considered browsing. Use of the GradLeaders USA, LLC. intranet is not considered browsing.

Tools To Compromise Systems Security—Unless specifically authorized by the Information Security department, GradLeaders USA, LLC. workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

Reporting Problems—Users must promptly report all information security alerts, warnings, and suspected vulnerabilities to the Information Systems department. Users must not use GradLeaders USA, LLC. systems to forward such information to other users, whether the other users are internal or external to GradLeaders USA, LLC.

Configuration Control

Changes To Application Software—GradLeaders USA, LLC. has a standard list of permissible software packages that users can run on their personal computers. Workers must not install other software packages on personal computers without obtaining advance permission from Information Systems department. Workers must not permit automatic software installation routines to be run on GradLeaders USA, LLC. personal computers unless these routines have been approved by the Information Systems department. Unless separate arrangements are made with the Information Systems department, upgrades to authorized software will be downloaded to personal computers automatically. Unapproved software may be removed without advance notice to the involved worker.

Changes To Operating System Configurations—On GradLeaders USA, LLC.-supplied computer hardware, workers must not change operating system configurations, upgrade existing operating systems, or install new operating systems. If such

changes are required, they must be performed by technical personnel, in person or with remote system maintenance software.

Changes To Hardware—Computer equipment supplied by GradLeaders USA, LLC. must not be altered or added to in any way without the prior knowledge of and authorization from the Information Systems department.

Access Control

Access Control Package—All GradLeaders USA, LLC. personal computers must run an access control package approved by the Information Security department. Typically these packages require a fixed password at the time a personal computer is booted and again after a certain period of no activity. Users must set the time frame for this period of no activity, at which point the contents of the screen are obscured, to 15 minutes or less. If sensitive information resides on a personal computer, the screen must immediately be protected with this access control package, or the machine turned off, whenever a worker leaves the location where the personal computer is in use.

Choice Of Passwords—The user-chosen passwords employed by access control software packages, and the keys employed by encryption packages, must be at least 8 characters in length. These passwords and keys must be difficult to guess. Words in a dictionary, derivatives of user IDs, and common character sequences such as "123456" must not be employed. Personal details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords and keys must not be any part of speech including, proper names, geographical locations, common acronyms, and slang.

Storage Of Passwords—Workers must maintain exclusive control of their personal passwords. They must not share them with others at any time. Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access controls, or in any other locations where unauthorized persons might discover them.

Encryption Of Secret Information—All computerized secret information must be encrypted when not in active use, for example, when not manipulated by software or viewed by an authorized user. The use of physical security measures such as safes, locking furniture, and locking office doors is recommended as a supplementary measure to protect secret information.

Logging Of Events Related To Secret Information—Personal computers handling secret information must securely log all significant computer security relevant events. Examples of computer security relevant events include password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software.

Physical Security

Donation Or Sale Of Equipment—Before personal computer equipment or storage media that has been used for GradLeaders USA, LLC. business is provided to any third party, the equipment or media must be physically inspected by the Information Security department to determine that all sensitive information has been removed. This policy does not apply when a non-disclosure agreement has been signed by the third party.

Lending Personal Computers To Others—Workers must never lend a GradLeaders USA, LLC. personal computer containing sensitive information to another person unless that other person has received prior authorization from the Owner if the sensitive information to access such information.

Custodians For Equipment—The primary user of a personal computer is considered a Custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a Custodian must promptly inform the involved department manager. With the exception of portable machines, personal

computer equipment must not be moved or relocated without the knowledge and approval of the involved department manager.

Use Of Personal Equipment—Workers must not bring their own computers, computer peripherals, or computer software into GradLeaders USA, LLC. facilities without prior authorization from their department head. Workers must not use their own personal computers for production GradLeaders USA, LLC. business unless these systems have been evaluated and approved by the Information Security department. Writing memos or reports is not considered production GradLeaders USA, LLC. business for purposes of this policy.

Positioning Display Screens—The display screens for all personal computers used to handle sensitive or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas. Care must also be taken to position keyboards so that unauthorized persons cannot readily see workers enter passwords, encryption keys, and other security-related parameters.

Locking Sensitive Information—When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.

Environmental Considerations—All personal computers in GradLeaders USA, LLC. offices must use surge suppressors. Those personal computers running production applications must also have uninterruptible power systems approved by the Information Security department.

Static Discharges And Electromagnetic Fields—If weather or building conditions pose a significant risk of static electricity discharge, personal computers must be outfitted with static protection equipment that has been approved by the Information Systems department. Magnetic storage media such as floppy disks and magnetic tapes must be kept at least several inches away from electric fields, such as those generated by magnets and a telephone when it rings.

Smoking, Eating, and Drinking—Workers must not smoke, eat, or drink when using personal computers.

Networking

Modems—Modems inside or attached to GradLeaders USA, LLC. office desktop personal computers are not permitted. Mobile and telecommuting personal computers are an exception to this rule. Communications software must always employ a password with at least 8 characters that has been constructed according to the rules found elsewhere in this document. When in GradLeaders USA, LLC. offices, users needing to make outbound connections with remote computers must route their connections through the Internet firewall.

Internet—As a matter of policy, inbound Internet connections to GradLeaders USA, LLC. personal computers is forbidden unless these connections employ an approved virtual private network (VPN) software package approved by the Information Security department. These VPN systems must employ both user authentication features with at least fixed passwords and data interception prevention features, such as encryption.

Downloading Sensitive Information—Sensitive GradLeaders USA, LLC. information may be downloaded from a multi-user system to a personal computer only if a clear business need exists, adequate controls to protect the information are currently installed on the involved personal computer, and advance permission from the information Owner has been obtained. This policy is not intended to cover electronic mail or memos, but does apply to databases, master files, and other information stored on servers, and other multi-user machines. This applies regardless of the media on which information is stored, the locations where the information is stored, the systems technology used to process the information, the people who handle it, or the processes by which information is handled.

Installation Of Communications Lines—Workers and vendors must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not obtained approval from the director of the Information Systems department.

Viruses

Virus Program Installed—All personal computers must continuously run the current version of virus detection package approved by the Information Security department. The current version of this virus package must be automatically downloaded to each personal computer when the machine is connected to the GradLeaders USA, LLC. internal network. Workers must not abort this download process. At a minimum, this package must execute whenever external storage media is supplied.

Decompression Before Checking—Externally-supplied floppy disks, CD-ROMs, and other removable storage media must not be used unless they have been checked for viruses. Attachments to electronic mail must not be executed or opened unless they have been checked for viruses. Externally-supplied, computer-readable files, software programs, databases, word processing documents, and spreadsheets must be decompressed prior to being subjected to an approved virus-checking process. If the files have been encrypted, they must be decrypted before running a virus-checking program.

Eradicating Viruses—Workers must not attempt to eradicate a virus without expert assistance. If workers suspect infection by a virus, they must immediately stop using the involved computer, physically disconnect from all networks, and contact the Information Systems department. If the suspected virus appears to be damaging information or software, workers must immediately turn off the personal computer.

Playing With Viruses—Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any GradLeaders USA, LLC. computer system.

Establishing Networks—Workers must not establish electronic bulletin boards, local area networks, modem connections to existing internal networks, Internet commerce systems, or other multi-user systems for communicating information without the specific approval of the Information Security department.

Automatic Device Synchronization—Systems that automatically exchange data between devices, such as a personal digital assistant and a personal computer, must not be enabled unless the systems have been evaluated and approved by the Information Security department.

Backup

Archival Copies—All personal computer software that is not standard GradLeaders USA, LLC. software must be copied prior to its initial usage, and such copies must be stored in a safe and secure location. These master copies, perhaps the media issued by the vendor, must not be used for ordinary business activities, but must be reserved for recovery from virus infections, hard disk crashes, and other computer problems. Documentation about the licenses for such software must be retained to get technical support, qualify for upgrade discounts, and verify the legal validity of the licenses.

Periodic Backup—All sensitive, valuable, or critical information resident on GradLeaders USA, LLC. computer systems must be periodically backed up. Such backup processes must be performed at least weekly. Unless automatic backup systems are known to be operational, all end users are responsible for making at least one current backup copy of sensitive, critical, or valuable files and storing that copy in a location on the local area network. These separate backup copies should be made each time that a significant number of changes are saved. Selected files from backups must be periodically restored to demonstrate the effectiveness of every backup process. Department managers must verify that proper backups are being made on all personal computers used for production business activities.

Reporting Software Purchases—All user department purchases of personal computer software that have not been handled through the Purchasing department must promptly be reported to the Information Systems department.

Copyright Protection—Making unauthorized copies of licensed and copyrighted software, even if for "evaluation" purposes, is forbidden. GradLeaders USA, LLC. permits reproduction of copyrighted materials only to the extent legally considered fair use or with the permission of the author or Owner. If workers have any questions about the relevance of copyright laws, they must contact corporate legal counsel. Unless they receive information to the contrary, workers must assume that software and other materials are copyrighted.

Destruction

Deletion of Old Information—Workers must delete information from their personal computers if it is clearly no longer needed or potentially useful. Prior to deleting any GradLeaders USA, LLC. information, workers should consult management to confirm such information is no longer necessary. Use of an erase feature is not sufficient for sensitive information because the information may be recoverable. Sensitive information should be deleted by an overwrite program approved by the Information Security department.

Destruction Of Information—Prior to disposal, defective or damaged floppy disks containing sensitive information must be destroyed using scissors or other methods approved by the Information Security department. Other storage media containing sensitive information must be disposed of in the locked destruction bins found in GradLeaders USA, LLC. offices. All hardcopy containing sensitive information must be disposed of in these bins or through an approved paper shredder.

Telecommuting & Mobile Computing

Management Issues

Telecommuting Privileges—Working at home or alternative site work arrangements, both known as telecommuting, are a management option, not a universal employee fringe benefit. Permission to telecommute is granted by an employee's manager. Before a telecommuting arrangement can begin, this manager must be satisfied that the job can be effectively performed off-site, that the worker has the personality and work habits suitable for telecommuting, and that an alternative work site is appropriate for the GradLeaders USA, LLC. tasks performed by the involved worker. Work site considerations include physical and information security for GradLeaders USA, LLC. property and a low-distraction work environment. Management also must be satisfied that the ways to measure worker performance are both clearly specified and realistic, and that the methods to stay in touch with other workers are adequate.

Periodic Privilege Reevaluation—The system privileges granted to all users, including the privilege to telecommute and to remotely access GradLeaders USA, LLC. systems, must be reevaluated by management every six months. Consistent compliance with the policies described in this document and related policies is an important factor in management's decision regarding the continuation of a telecommuting arrangement. Related policies include, but are not limited to, compliance with software license agreements and reporting suspected computer virus infections. Many related policies are not reiterated here because they appear in other GradLeaders USA, LLC. policies. This policy is restricted to security matters relevant to telecommuters and mobile computer users.

Work Site Inspections—GradLeaders USA, LLC. maintains the right to conduct physical inspections of telecommuter offices without advance notice. GradLeaders USA, LLC. also maintains the right to examine the contents of any computer that contains or is thought to contain GradLeaders USA, LLC. internal information, including computers that have been purchased by employees, contractors, consultants, temporaries, and others. GradLeaders USA, LLC. additionally retains the right to remotely inspect the contents of and configuration of computers used by telecommuters, through remote systems administration tools.

Consistent Security—GradLeaders USA, LLC. information must at all times be protected in a manner commensurate with its sensitivity and criticality. The precautions described in this policy apply regardless of the storage media on which information is recorded, the locations where the information is stored, the systems used to process the information, the individuals who have access to the information, or the processes by which the information is handled. This means that workers must protect information in a similar manner no matter whether they are in a GradLeaders USA, LLC. office, a hotel room, or at a home office.

Intellectual Property Rights—Intellectual property developed or conceived of while a worker is attending to GradLeaders USA, LLC. business at an alternative work site is the exclusive property of GradLeaders USA, LLC. Such intellectual property includes patent, copyright, trademark, and all other intellectual property rights as manifested in memos, plans, strategies, products, computer programs, documentation, and other GradLeaders USA, LLC. materials.

Reporting Loss or Damage—Workers at remote working locations must promptly report to their manager any damage to or loss of GradLeaders USA, LLC. computer hardware, software, or sensitive information that has been entrusted to their care.

Access Control

Encryption And Boot Protection—All computers used for telecommuting, and portables, laptops, notebooks, and other transportable computers containing sensitive (Confidential or Secret) GradLeaders USA, LLC. information must consistently employ both hard disk encryption for all data files and boot protection through a password. These two essential controls must be provided through software or hardware systems approved by the Information Security department. Personal digital assistants, handheld computers, and smart phones must not be used to handle GradLeaders USA, LLC. sensitive information unless they have been configured with the necessary controls, such as encryption and boot protection, and approved for such use by the Information Systems department. Exceptions will be made for calendars, address books, and stored connection information such as telephone numbers.

Sharing Access Devices and Systems—Telecommuters must not share dynamic password token cards, smart cards, fixed passwords, or any other access devices or parameters with anyone without prior approval from the Information Security department. This means that a remote computer used for GradLeaders USA, LLC. business must be used exclusively by the telecommuter. Family members, friends, and others must not be permitted to use this machine. Telecommuters must never lend to others a handheld computer, a personal digital assistant, a smart phone, or any other computer that stores information about GradLeaders USA, LLC. business activities.

Physical Security

Similarity In Approaches—At alternative work sites, reasonable precautions must be taken to protect GradLeaders USA, LLC. hardware, software, and information from theft, damage, and misuse.

Provision Of Secure Containers—Workers who must keep Secret or Confidential GradLeaders USA, LLC. information at their homes in order to do their work must have safes or lockable heavy furniture for the proper storage of this information.

Shredders—Telecommuters must have or be provided with a shredder to appropriately dispose of printed versions of sensitive information. Shredders that make strips of paper are not acceptable for the disposal of GradLeaders USA, LLC. sensitive material. Acceptable shredders make confetti or other small particles. All sensitive GradLeaders USA, LLC. paper-resident information plus any information containing financial account numbers, like credit card numbers, must be shredded. Intermediate work products containing sensitive information, such as carbon copies, photocopies, photographic negatives, or paper memo drafts, must also be shredded. Telecommuting workers on the road must not throw away GradLeaders USA, LLC. sensitive information in hotel wastebaskets or other publicly-accessible trash containers. Sensitive information must be retained until it can be shredded, or destroyed with other approved methods.

Moving Residence Location—If a telecommuting worker has an intention to move his or her residence or off-site work location to another site, the worker must notify his or her manager and get approval prior to the move. The worker also must follow Information Security department instructions associated with telecommuter residence moves. The new location must meet all the current telecommuter site requirements.

Screen Positioning—The display screens for all systems used to handle GradLeaders USA, LLC. sensitive information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.

Logging-Out—After a worker has completed a remote session with GradLeaders USA, LLC. computers, the worker must log off and then hang up, rather than only hanging up. Workers using remote communications facilities must wait until they receive a confirmation of their log off command from the remotely connected GradLeaders USA, LLC. machine before they leave the computer they are using.

Communications Links

Establishing Dial-Up Facilities—Workers must not leave their personal computers unattended with a modem turned on and communications software enabled unless they have installed an access control system approved by the Information Security department. Workers must not establish any communications systems that ordinarily accept in-coming dial-up calls unless these systems have been approved by an Information Security manager.

Inbound Dial-Up to GradLeaders USA, LLC. Networks—All in-bound dial-up lines connected to GradLeaders USA, LLC. internal networks and networked computer systems must pass through an additional access control point, such as a firewall, telecommunications front end, or similar system, before users are permitted to reach an operating system-based computer logon screen asking for a user ID and fixed password. This additional access point must employ dynamic passwords or another extended user authentication technology approved by the Information Security department.

Establishing Internet Connections—Workers must not establish firewalls, routers, communications servers, or any other facilities on their remote computer systems that handle GradLeaders USA, LLC. business if these facilities permit telnet or any other type of real-time inbound remote access through the Internet. Outbound connections from a remote system through the Internet, terminating at a GradLeaders USA, LLC. networked computer system, are permissible as long as these connections are secured by a virtual private network software package.

Other Connections—Other than dial-up and Internet connections, workers must not establish any other interface between a remote computer used for GradLeaders USA, LLC. business activities and another network, such as value-added networks, unless prior approval of the Information Security department has been obtained in writing. This means that workers are prohibited from establishing their own personal accounts with Internet service providers and using these accounts for GradLeaders USA, LLC. business. Instead, all GradLeaders USA, LLC. business Internet electronic mail and Internet surfing must be accomplished through a GradLeaders USA, LLC.-managed firewall with GradLeaders USA, LLC. approved electronic mail software.

DSL Lines And Cable Modem Lines—Digital subscriber lines, cable modem lines, and other high-speed lines must not be used for any GradLeaders USA, LLC. business communications unless a firewall and an approved virtual private network is employed. Telecommuters must contact the Information System department for assistance in the establishment of these facilities before making any arrangements with third-party vendors.

Radio Networks—Workers transmitting sensitive GradLeaders USA, LLC. information must not employ radio networks, such as cellular modems, unless these network channels are encrypted. The use of digital communications protocols rather than traditional analog communications protocols does not qualify as encryption.

Telephone Discussions—Workers must take steps to avoid discussing sensitive information when on the telephone. If discussion of such information is absolutely required, workers must use guarded terms and refrain from mentioning sensitive details beyond those needed to get the job done. Secret information must not be discussed on speakerphones

unless all participating parties acknowledge that no unauthorized persons are in close proximity such that they might overhear the conversation. Unless an encryption system approved by the Information Security department is used, secret GradLeaders USA, LLC. information must never be discussed on cordless or cellular telephones.

Voice Mail Systems —Unless the receiving voice mail system is known to be password protected, workers must refrain from leaving messages containing sensitive information on these recording systems. Unless their voice mail system is password protected, telecommuting workers must record an outgoing message informing callers that their incoming message recording system is not secure and is not suitable for sensitive information.

Backup And Media Storage

Backup—Telecommuters are responsible for ensuring that their remote systems are backed up on a periodic basis, either automatically through the network or remotely with tape drives or similar equipment. If backups are made locally, telecommuting workers must store copies of these same backups at a secure location away from the remote working site at least every two weeks. If these backups contain sensitive information, the backups must be encrypted using software approved by the Information Security department.

Sensitive Media Marking and Storage—When sensitive information is written to a floppy disk, magnetic tape, CD-RW or other storage media, the media must be externally marked with the highest relevant sensitivity classification. Unless encrypted, when not in use, this media must be stored in heavy locked furniture. Smart cards and tamper-resistant security modules are an exception to this rule.

Automatic Device Synchronization—Systems that automatically exchange data between devices, such as the file synchronization mechanism used with a personal digital assistant and a personal computer, must not be enabled unless the systems have been evaluated and approved by the Information Security department.

Setting Date and Time—Telecommuting workers must diligently keep their remote computers' internal clocks synchronized to the actual date and time.

System Management

GradLeaders USA, LLC.-Provided Machines—Employees working on GradLeaders USA, LLC. business at alternative work sites must use GradLeaders USA, LLC.-provided computer and network equipment. An exception will be made only if other equipment has been approved by the Information System department as compatible with GradLeaders USA, LLC. information systems and controls.

Telecommuting Systems—Workers attending to GradLeaders USA, LLC. business at alternative work sites must use only GradLeaders USA, LLC.-provided computer software, hardware, and network equipment. An exception will be made only if other systems have been approved by the Information Systems department as compatible with GradLeaders USA, LLC. information systems and controls. Workers should not bring personally-owned computers into GradLeaders USA, LLC. offices to process or otherwise handle GradLeaders USA, LLC. information without prior approval from the Information Systems department.

Changes to Configurations And Software—On GradLeaders USA, LLC.-supplied computer hardware, workers must not change the operating system configuration or install new software. If such changes are required, they must be performed by Information System personnel with remote system maintenance software. Changing the font defaults for a word processing program, or otherwise altering the templates provided with an application, is permissible without Help Desk assistance or advance approval.

Changes to Hardware—Computer equipment supplied by GradLeaders USA, LLC. must not be altered or added to in any way without prior knowledge and authorization from the Information System department.

Downloading Software—Without prior authorization, workers must not download software from dial-up electronic bulletin board systems, the Internet, or other systems outside GradLeaders USA, LLC. onto computers used to handle GradLeaders USA, LLC. data.

Ownership Versus Possession—If GradLeaders USA, LLC. supplied a telecommuter with software, hardware, furniture, information or other materials to perform GradLeaders USA, LLC. business remotely, the title to, and all rights and interests to these items will remain with GradLeaders USA, LLC. In such instances, telecommuter possession does not convey ownership or any implication of ownership. All such items must be promptly returned to GradLeaders USA, LLC. when a telecommuter separates from GradLeaders USA, LLC., or when so requested by the telecommuter's manager.

Liability For GradLeaders USA, LLC. Property—If GradLeaders USA, LLC. supplied a telecommuter with software, hardware, furniture, information or other materials to perform GradLeaders USA, LLC. business remotely, GradLeaders USA, LLC. assumes all risks of loss or damage to these items unless such loss or damage occurs due to the telecommuter's negligence. GradLeaders USA, LLC. expressly disclaims any responsibility for loss or damage to persons or property caused by, or arising out of the usage of such items.

Electromagnetic Interference—In some cases, use of computers or other electronic devices will generate electromagnetic interference that will affect televisions, radios, or other machines. If a telecommuting system set-up to perform GradLeaders USA, LLC. business generates such interference, its use must be terminated immediately until such time as the specific nature of and a solution for the problem has been identified.

Travel Considerations

Removal Of Information—Sensitive (Confidential or Secret) information may not be removed from GradLeaders USA, LLC. premises unless the information's Owner has approved in advance. This policy includes sensitive information stored on portable computer hard disks, floppy disks, CD-ROMs, magnetic tape cartridges, and paper memos. An exception is made for authorized off-site backups that are in encrypted form.

Traveling with Secret Information—Unless specific approval from a local department manager has been granted, workers must avoid traveling on public transportation when in the possession of Secret GradLeaders USA, LLC. information.

Foreign Transport—Whenever Secret information is carried by a GradLeaders USA, LLC. worker into a foreign country, the information must either be stored in some inaccessible form, such as an encrypted floppy disk, or must remain in the worker's possession at all times. GradLeaders USA, LLC. workers must not take Secret GradLeaders USA, LLC. information into another country unless the permission has been obtained from Information Security management.

Public Exposure—Sensitive GradLeaders USA, LLC. information must not be read, discussed, or otherwise exposed in restaurants, on airplanes, on trains, or in other public places where unauthorized people might discover it.

Checked Luggage—Workers in the possession of portable, laptop, notebook, palmtop, handheld, smart phones, personal digital assistants, and other transportable computers containing sensitive GradLeaders USA, LLC. information must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler as hand luggage.

Securing Hardcopy Sensitive Information—Whenever a hardcopy version of Secret information is removed from GradLeaders USA, LLC. premises, it must either be stored in a safe, locking furniture, or some other heavy container with a lock, or carried in a locked briefcase when not in use. Such information must not be left in an unattended motor vehicle, hotel room, or external office, even if this vehicle or room is locked.

Faxing Sensitive Information—If secret information is sent by fax, the recipient must have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception will be made if the area surrounding the fax machine is physically restricted such that persons who are not authorized to see the material being faxed may not enter. This means that sensitive

GradLeaders USA, LLC information must not be faxed through a hotel desk or other untrusted third parties. Another exception will be made in those instances in which the destination fax machine is password protected and authorized parties are the only ones who have access to the involved password.

Electronic Mail

Company Property—As a productivity enhancement tool, GradLeaders USA, LLC. encourages the business use of electronic communications systems, notably the Internet, telephone, pager, voice mail, electronic mail, and fax. Unless third parties have clearly noted copyrights or some other rights on the messages handled by these electronic communications systems, all messages generated on or handled by GradLeaders USA, LLC. electronic communications systems are considered to be the property of GradLeaders USA, LLC.

Authorized Usage—GradLeaders USA, LLC. electronic communications systems generally must be used for business activities only. Incidental personal use is permissible as long as it does not consume more than a trivial amount of system resources, does not interfere with worker productivity, and does not preempt any business activity. GradLeaders USA, LLC. electronic communication systems must not be used for charitable fund raising campaigns, political advocacy efforts, religious efforts, private business activities, or personal amusement and entertainment. News feeds, electronic mail mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to both GradLeaders USA, LLC. business and the duties of the receiving workers. Workers are reminded that the use of corporate information system resources must never create the appearance or the reality of inappropriate use.

Default Privileges—Electronic communication systems must be established and maintained such that only the privileges necessary to perform a job are granted to a worker. For example, when a worker's relationship with GradLeaders USA, LLC. comes to an end, all of the worker's privileges on GradLeaders USA, LLC. electronic communications systems also must cease. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of a department manager has been obtained.

User Separation—Where electronic communications systems provide the ability to separate the activities of different users, these facilities must be implemented. Electronic mail systems must employ personal user IDs and secret passwords to isolate the communications of different users. Workers must not employ the user ID or the identifier of any other user.

User Accountability—Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. Information Technology Department staff must never ask users to reveal their passwords. If users need to share computer resident data, they should utilize message forwarding facilities, public directories on local area network servers, groupware databases, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess. For example, users must not choose a dictionary word, details of their personal history, a common name, or a word that reflects work activities.

User Identity—Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings. Workers must not send anonymous electronic communications. At a minimum, all workers must provide their name and phone number in all electronic communications. Electronic mail signatures indicating job title, company affiliation, address, and other particulars are strongly recommended for all electronic mail messages.

Use Only GradLeaders USA, LLC. Electronic Mail Systems—Unless permission from the Information Security Manager has first been obtained, workers must not use their personal electronic mail accounts with an Internet service provider or any other third party for any GradLeaders USA, LLC. business messages. To do so would circumvent logging, virus checking,

content screening, and automated backup controls that GradLeaders USA, LLC. has established. Likewise, workers must not use the electronic mail features found in web browsers for any GradLeaders USA, LLC. business communications. They must instead employ only authorized GradLeaders USA, LLC. electronic mail software.

Use Of Encryption Programs—Workers are reminded that GradLeaders USA, LLC. electronic communications systems are not encrypted by default. If sensitive information (classified as Confidential or Secret) must be sent by electronic communication systems, an encryption process approved by the Information Security Department must be employed. These encryption systems must protect the sensitive information from end to end (from sender to recipient). In other words, they must not involve decryption of the message content before the message reaches its intended final destination. Mobile computers, notebook computers, portable computers, personal digital assistants, and similar computers that store GradLeaders USA, LLC. sensitive information must consistently employ file encryption to protect this sensitive information when it is stored inside these same computers, and when it is stored on accompanying data storage media. Users of these types of computers who are recipients of sensitive information sent by electronic mail must delete this information from their systems if they do not have encryption software that can properly protect it. Separately, workers must not use encryption for any production electronic communications system unless a backup key or a key escrow system has been established with the cooperation of the Information Security Department.

Labeling Electronic Mail Messages—All electronic mail messages containing sensitive information must include the appropriate classification (Confidential or Secret) in the header. This label will remind recipients that the information must not be disseminated further, or be used for unintended purposes, without the proper authorization.

Respecting Intellectual Property Rights—Although the Internet is an informal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. Workers using GradLeaders USA, LLC. electronic mail systems must repost or reproduce material only after obtaining permission from the source, quote material from other sources only if these other sources are properly identified, and reveal internal GradLeaders USA, LLC. information on the Internet only if the information has been officially approved for public release. All information acquired from the Internet must be considered suspect until confirmed by another source. There is no quality control process on the Internet, and a considerable amount of information posted on the Internet is outdated, inaccurate, and/or deliberately misleading.

Respecting Privacy Rights—Except as otherwise specifically approved by the Information Security Manager, workers must not intercept or disclose, or assist in intercepting or disclosing, electronic communications. GradLeaders USA, LLC. is committed to respecting the rights of its workers, including their reasonable expectations of privacy. GradLeaders USA, LLC. is also responsible for operating, maintaining, and protecting its electronic communications networks. To accomplish these objectives, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications. To meet these objectives, GradLeaders USA, LLC. may employ content monitoring systems, message logging systems, and other electronic system management tools. By making use of GradLeaders USA, LLC. systems, users consent to permit all information they store on GradLeaders USA, LLC. systems to be divulged to law enforcement at the discretion of GradLeaders USA, LLC. management.

No Guaranteed Message Privacy—GradLeaders USA, LLC. cannot guarantee that electronic communications will be private. Workers must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Electronic communications can be accessed by people other than the intended recipients in accordance with this policy. Because messages can be stored in backups, electronic communications actually may be retrievable when a traditional paper letter would have been discarded or destroyed. Workers must accordingly be careful about the topics covered in GradLeaders USA, LLC. electronic communications, and should not send a message discussing anything that they would not be comfortable reading about on the front page of their local newspaper.

Contents Of Messages—Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. It is possible that these remarks would later be taken out of context and used against GradLeaders USA, LLC. To prevent these problems, workers must concentrate on business

matters in GradLeaders USA, LLC. electronic communications. As a matter of standard business practice, all GradLeaders USA, LLC. electronic communications must be consistent with conventional standards of ethical and polite conduct (no "flaming" is allowed).

Incidental Disclosure—It may be necessary for technical support personnel to review the content of an individual worker's communications during the course of problem resolution. These staff members must not review the content of an individual worker's communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels. Advance approval by the Information Security Manager is required for all such monitoring.

Addendum On Outbound Electronic Mail—A footer prepared by the Information Security Department must be automatically appended to all outbound electronic mail originating from GradLeaders USA, LLC. computers. This footer must make reference to the possibility that the message may contain confidential information, that it is for the use of the named recipients only, that the message has been logged for archival purposes, that the message may be reviewed by parties at GradLeaders USA, LLC. other than those named in the message header, and that the message does not necessarily constitute an official representation of GradLeaders USA, LLC.

Handling Attachments—When sending an attachment to a third party, workers must attempt to use rich text format (RTF) or simple text files whenever possible. This is because attachments to electronic mail messages, if they have any executable code embedded in them, may contain a virus or may in some other way damage a worker's computer. Workers must encourage third parties to send them files in these same two formats whenever reasonable and practical. All other attachment files must be scanned with an authorized virus detection software package before opening or execution. In some cases, attachments must be decrypted or decompressed before a virus scan takes place. Workers must be suspicious about unexpected electronic mail attachments received from third parties, even if the third party is known and trusted.

Message Forwarding—Electronic communications users must exercise caution when forwarding messages. GradLeaders USA, LLC. sensitive information such as Confidential or Secret must not be forwarded to any party outside GradLeaders USA, LLC. without the prior approval of a local department manager. Blanket forwarding of messages to parties outside GradLeaders USA, LLC. is prohibited unless the prior permission of the Information Security Manager has been obtained. Messages sent by outside parties must not be forwarded to other third parties unless the sender clearly intended this and such forwarding is necessary to accomplish a customary business objective. In all other cases, forwarding of messages sent by outsiders to other third parties can be done only if the sender expressly agrees to this forwarding.

Handling Alerts About Security—Users must promptly report all information security alerts, warnings, and reported vulnerabilities to the Information Security Department. Information Security is the only organizational unit authorized to determine appropriate action in response to such notices. Users must not utilize GradLeaders USA, LLC. systems to forward these notices to other users, whether the other users are internal or external to GradLeaders USA, LLC. Users must promptly report all suspected security vulnerabilities or problems that they notice to Information Security.

Public Representations—No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about GradLeaders USA, LLC. may be issued unless it has been approved by the Marketing Department. GradLeaders USA, LLC., as a matter of policy, does not send unsolicited electronic mail, nor does it issue unsolicited fax advertising. Nobody outside GradLeaders USA, LLC. may be placed on an electronic mail distribution list without indicating their intention to be included on the list through an opt-in process. If GradLeaders USA, LLC. workers are bothered by an excessive amount of unwanted messages from a particular organization or electronic mail address, they must not respond directly to the sender. Recipients must forward samples of the messages to the system administrator in charge of the electronic mail system for resolution. Workers must not send large number of messages in order to overload a server or user's electronic mailbox in retaliation for any perceived issue.

User Backup—If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a GradLeaders USA, LLC. management decision, it must be retained for future reference. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail inboxes must not be used for the archival storage of important information.

Purging Electronic Messages—Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After six months of electronic mail messages are stored on GradLeaders USA, LLC. mail servers, they must be automatically deleted by systems administration staff.

Harassing Or Offensive Materials—GradLeaders USA, LLC. computer and communications systems are not intended to be used for, and must not be used for the exercise of the workers' right to free speech. These systems must not be used as an open forum to discuss GradLeaders USA, LLC. organizational changes or business policy matters. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Workers who receive offensive unsolicited material from outside sources must not forward or redistribute it to either internal or external parties, unless this forwarding or redistribution is to the GradLeaders USA, LLC. Information Security Department in order to assist with the investigation of a complaint.

Responding Directly To The Sender—Workers must respond directly to the originator of offensive electronic mail messages, telephone calls, or other electronic communications. If the originator does not promptly stop sending offensive messages, workers must report the communications to their manager and the Information Security Department. GradLeaders USA, LLC. retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Use At Your Own Risk—Workers access the Internet with GradLeaders USA, LLC. facilities at their own risk. GradLeaders USA, LLC. is not responsible for material viewed, downloaded, or received by users through the Internet. Electronic mail systems may deliver unsolicited messages that contain offensive content.

Establishing Electronic Business Systems—Although GradLeaders USA, LLC. implements electronic data interchange (EDI), Internet commerce, and other electronic business systems with third parties, all contracts must be formed by paper documents prior to purchasing or selling through electronic systems. EDI, electronic mail, and similar binding business messages must be releases against blanket orders, such as a blanket purchase order. All electronic commerce systems must be approved by the chief information officer and the Information Security Manager prior to usage.

Paper Confirmation For Contracts—All contracts formed through electronic offer and acceptance messages must be formalized and confirmed through paper documents within two weeks of acceptance. Workers must not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.

Internet

Introduction

Opportunities and Risks—The wide array of new resources, services, and inter-connectivity available through the Internet all introduce new business opportunities, and new security and privacy risks. In response to the risks, this policy describes the GradLeaders USA, LLC. official policy regarding Internet security.

Applicability—This policy applies to all workers, employees, contractors, consultants, temporaries, and volunteers, who use the Internet with GradLeaders USA, LLC. computing or networking resources. The policy applies to all those who use the Internet and represent themselves as being connected in some way with GradLeaders USA, LLC. All of these Internet users are expected to be familiar with and fully comply with this policy. Questions about the policy should be directed to the Information Security department. Violations of this policy can lead to revocation of system privileges or additional disciplinary action up to and including termination.

Access —Access to the Internet, aside from electronic mail, will be provided to only those workers who have a legitimate business need for such access. The ability to access the Internet and engage in other Internet activities is not a fringe benefit to which all workers are entitled.

Information Integrity

Information Reliability—All information acquired from the Internet must be considered suspect until confirmed by separate information from another source. Before using free Internet-supplied information for business decision-making purposes, workers must corroborate the information by consulting other sources.

Virus Checking—All non-text files downloaded from non-GradLeaders USA, LLC. sources through the Internet must be screened with current virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software must be tested on a stand-alone, non-production machine that has been recently backed up. Downloaded files must be decrypted and decompressed before being screened for viruses. The use of digital signatures to verify that a file has not been altered by unauthorized parties is recommended, but this does not assure freedom from viruses, Trojan horses, and other problems.

Push Technology—Automatic updating of software or information on GradLeaders USA, LLC. computers through background push Internet technology is prohibited unless the involved vendor's system has been tested and approved by the Internet group within the Information Systems department.

Spoofing Users—Before workers release any internal GradLeaders USA, LLC. information, enter into any contracts, or order any products through public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed through digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third-party references, and telephone conversations may be used.

User Anonymity—Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any GradLeaders USA, LLC. electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. Use of anonymous FTP logons, anonymous UUCP logons, HTTP or web browsing, and other access methods established with the expectation that users would be anonymous are permissible.

Web Page Changes—Workers must not establish new Internet pages dealing with GradLeaders USA, LLC. business, or make modifications to existing web pages dealing with GradLeaders USA, LLC. business, unless they have obtained the approval of their department manager. Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page. Management must ensure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected with adequate security measures.

Web Page Archives—Every version of the GradLeaders USA, LLC. Internet site and commerce site files must be securely archived in two physically separated locations. The technology department will designate a web master who will keep this archive and provide copies of historical pages on demand.

Information Confidentiality

Information Exchange—GradLeaders USA, LLC. software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-GradLeaders USA, LLC. party for any purposes other than business purposes expressly authorized by management. Exchanges of software or data between GradLeaders USA, LLC. and any third party must not proceed unless a written agreement has been signed. Such an agreement must specify the terms of the exchange, and the ways that the software or data is to be handled and protected. Regular business practices, such as shipment of a product in response to a customer purchase order, need not involve such a specific agreement since the terms and conditions are implied.

Posting Materials—Workers must not post unencrypted GradLeaders USA, LLC. material on any publicly-accessible Internet computer that supports anonymous FTP or similar publicly-accessible services, unless the posting of these

materials has been approved by management. GradLeaders USA, LLC. internal information must not be placed in any computer unless the persons who have access to that computer have a legitimate business need to know the involved information.

Message Interception—GradLeaders USA, LLC. secret, proprietary, or private information must not be sent over the Internet unless it has been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet. For the same reasons, Internet telephone services must not be used for GradLeaders USA, LLC. business unless the connection is known to be encrypted.

Security Parameters—Unless a connection is known to be encrypted, credit card numbers, telephone calling card numbers, fixed logon passwords, and other security parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form. Encryption processes are permissible if they are approved by the Information Security manager.

Public Representations

External Representations—Workers may indicate their affiliation with GradLeaders USA, LLC. in mailing lists, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for example through an electronic mail address. In either case, whenever workers provide an affiliation, unless they have been expressly designated as a spokesperson of GradLeaders USA, LLC., they also must clearly indicate the opinions expressed are their own, and not necessarily those of GradLeaders USA, LLC. If an affiliation with GradLeaders USA, LLC. is provided, political advocacy statements and product or service endorsements also are prohibited. With the exception of ordinary marketing and customer service activities, all representations on behalf of GradLeaders USA, LLC. must be cleared by management.

Appropriate Behavior—Whenever any affiliation with GradLeaders USA, LLC. is included with an Internet message or posting, written attacks are strictly prohibited. Workers must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

Removal Of Postings—Those messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, that include an implied or explicit affiliation with GradLeaders USA, LLC., may be removed if management deems them to be inconsistent with GradLeaders USA, LLC. business interests or existing company policy. Messages in this category include political statements, religious statements, cursing or other foul language, and statements viewed as harassing others based on race, creed, color, age, sex, physical handicap, or sexual orientation. The decision to remove electronic mail must be made by the corporate Information Security manager. When practical and feasible, individuals responsible for the message will be informed of the decision and given the opportunity to remove the message themselves.

Disclosing Internal Information—Workers must not publicly disclose internal GradLeaders USA, LLC. information through the Internet that may adversely affect the GradLeaders USA, LLC. customer relations or public image unless the approval of a member of the top management team has been obtained. Such information includes business prospects, products now in research and development, product performance analyses, product release dates, and internal information systems problems. Responses to specific customer electronic mail messages are exempted from this policy.

Inadvertent Disclosure—Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Usenet, and related public postings on the Internet. Before posting any material, workers must consider whether the posting could put GradLeaders USA, LLC. at a significant competitive disadvantage or whether the material could cause public relations problems. Workers should keep in mind that several separate pieces of information can be pieced together by a competitor to form a picture revealing confidential information that then could be used against GradLeaders USA, LLC. Workers must never post on the Internet the specific computer or network products employed by GradLeaders USA, LLC.

Intellectual Property Rights

Copyrights—When at work, or when GradLeaders USA, LLC. computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with GradLeaders USA, LLC. work, and are therefore prohibited. The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author or Owner. Workers must assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" and specifics about the source of the information.

Publicly-Writable Directories—All publicly-writable directories on GradLeaders USA, LLC. Internet-connected computers must be reviewed and cleared each evening. Workers using GradLeaders USA, LLC. computers must not be involved in any way with the exchange of pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material.

Access Control

Inbound User Authentication—All users wishing to establish a real-time connection with GradLeaders USA, LLC. internal computers through the Internet must employ a virtual private network (VPN) product approved by the Information Security department that can encrypt all traffic exchanged. These VPN products also must authenticate remote users at a firewall before permitting access to the GradLeaders USA, LLC. internal network. This authentication process must be achieved through a dynamic password system approved by the corporate Information Security manager. Examples of approved technology include hand-held smart cards with dynamic passwords and user-transparent challenge and response systems. Designated public systems do not need user authentication processes because anonymous interactions are expected.

Remote Machine Security—Workers who have not installed required software patches or upgrades, or whose systems are virus-infested must be disconnected automatically from the GradLeaders USA, LLC. network until they have reestablished a secure computing environment. The computers used by all workers employing VPN technology must be remotely scanned automatically to determine that the software is current and that the system has been properly secured.

Restriction Of Third-Party Access—Inbound Internet access privileges must not be granted to third-party vendors, contractors, consultants, temporaries, outsourcing organization personnel or other third parties unless the relevant system manager determines that these individuals have a legitimate business need for such access. These privileges must be enabled only for specific individuals and only for the time period required to accomplish approved tasks.

Browser User Authentication—Workers must not save fixed passwords in their web browsers or electronic mail clients. These fixed passwords must be provided each time that a browser or electronic mail client is invoked. Browser passwords may be saved if a boot password must be provided each time the computer is powered up, and if a screen saver password must be provided each time the system is inactive for a specified period of time. GradLeaders USA, LLC. computer users must refuse all offers by software to place a cookie on their computer so that they can automatically log on the next time that they visit a particular Internet site. Cookies that serve other purposes are permissible.

Data Aggregators—Workers must not provide their Internet user IDs and passwords to data aggregators, data summarization and formatting services, or any other third parties.

Internet Service Providers—With the exception of telecommuters and mobile computer users, workers must not employ Internet service provider accounts and dial-up lines to access the Internet with GradLeaders USA, LLC. computers. All Internet activity must pass through GradLeaders USA, LLC. firewalls so that access controls and related security mechanisms can be applied. Users must employ their GradLeaders USA, LLC. electronic mail address for Internet electronic mail. Use of a personal electronic mail address for this purpose is prohibited.

Establishing Network Connections—Unless the prior approval of the manager of Internet Services has been obtained, workers must not establish Internet or other external network connections that could permit non-GradLeaders USA, LLC. users to gain access to GradLeaders USA, LLC. systems and information. These connections include the establishment of multi-computer file systems, Internet pages, Internet commerce systems, and FTP servers.

Conducting Business Over The Internet—Unless advance approval of the Purchasing department has been obtained, GradLeaders USA, LLC. workers must not purchase any goods or services through the Internet if these goods or services are offered by a business based in, or operating out of, a foreign country.

Personal Use

Personal Use—Workers who have been granted Internet access who wish to explore the Internet for personal purposes must do so on personal rather than company time. Games, news groups, and other non-business activities must be performed on personal, not company time. Use of GradLeaders USA, LLC. computing resources for these personal purposes is permissible as long as the incremental cost of the usage is negligible, no GradLeaders USA, LLC. business activity is preempted by the personal use, and the usage is not likely to cause either a hostile working environment or a poor behavioral example. Workers must not employ the Internet or other internal information systems in such a way that the productivity of other workers is eroded. Examples of this include chain letters and broadcast charitable solicitations. GradLeaders USA, LLC. computing resources must not be resold to other parties or used for any personal business purposes such as running a consulting business on off-hours.

Offensive Web Sites—GradLeaders USA, LLC. is not responsible for the content that workers may encounter when they use the Internet. When and if users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session. Workers using GradLeaders USA, LLC. computers who discover they have connected with a web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.

Blocking Sites and Content Types—The ability to connect with a specific web site does not in itself imply that users of GradLeaders USA, LLC. systems are permitted to visit that site. GradLeaders USA, LLC. may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include graphic and music files.

Privacy Expectations

No Default Protection—Workers using GradLeaders USA, LLC. information systems or the Internet must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers must not send information over the Internet if they consider it to be confidential or private.

Management Review—At any time and without prior notice, GradLeaders USA, LLC. management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through GradLeaders USA, LLC. computers.

Logging—GradLeaders USA, LLC. routinely logs the web sites visited, files downloaded, time spent on the Internet, and related information. Department managers receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

Junk Electronic Mail—Users must not use GradLeaders USA, LLC. computer systems for the transmission of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients. These prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters,

pyramid schemes, and direct marketing pitches. When workers receive unwanted and unsolicited electronic mail, they must refrain from responding directly to the sender. They must forward the message to the electronic mail administrator at GradLeaders USA, LLC. who then can take steps to prevent further transmissions.

Reporting Security Problems

Notification Process—If sensitive GradLeaders USA, LLC. information is lost, disclosed to unauthorized parties, or suspected of either, the Information Security manager must be notified immediately. If any unauthorized use of GradLeaders USA, LLC. information systems has or is suspected of taking place, the Information Security manager must be notified immediately. Whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Information Security manager must be notified immediately. All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages must be immediately reported to the Information Security department. The specifics of security problems must not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports—Workers in receipt of information about system vulnerabilities must forward it to the Information Security manager, who then will determine what if any action is appropriate. Workers must not personally redistribute system vulnerability information to other users.

Testing Controls—Workers must not test or probe security mechanisms at either GradLeaders USA, LLC. or other Internet sites unless they have obtained written permission from the Information Security manager. The possession or the usage of tools for detecting information system vulnerabilities, or tools for compromising information security mechanisms, are prohibited without the advance permission of the corporate Information Security manager.

Glossary

Access control: A system to restrict the activities of users and processes based on the need to know.

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Algorithm: A mathematical process for performing a certain calculation. In the information security field, it is generally used to refer to the process for performing encryption.

Badge reader: A device that reads worker identity badges and interconnects with a physical access control system that may control locked doors.

Booting: The process of initializing a computer system from a turned-off or powered-down state.

Bridge: A device that interconnects networks or that otherwise permits networking circuits to be connected.

Compliance statement: A document used to obtain a promise from a computer user that such user will abide by system policies and procedures.

Confidential information: A sensitivity designation for information, the disclosure of which is expected to damage GradLeaders USA, LLC. or its business affiliates.

Critical information: Any information essential to GradLeaders USA, LLC. business activities, the destruction, modification, or unavailability of which would cause serious disruption to GradLeaders USA, LLC. business.

Cryptographic challenge and response: A process for identifying computer users involving the issuance of a random challenge to a remote workstation, which is then transformed using an encryption process and a response is returned to the connected computer system.

Default file permission: Access control file privileges, read, write, execute, and delete, granted to computer users without further involvement of either a security administrator or users.

Default password: An initial password issued when a new user ID is created, or an initial password provided by a computer vendor when hardware or software is delivered.

Dynamic password: A password that changes each time a user logs on to a computer system.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

Encryption: A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives.

End User: A user who employs computers to support GradLeaders USA, LLC. business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process typically achieved by user IDs and fixed passwords, such as hand-held tokens and dynamic passwords.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have passed some security check, such as providing a password.

Front-end processor (FEP): A small computer used to handle communications interfacing for another computer.

Gateway: A computer system used to link networks that can restrict the flow of information and that employ some access control method.

Hand-held token: A commercial dynamic password system that employs a smart card to generate one-time passwords that are different for each session.

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the time frames that these types of information must be kept.

Isolated computer: A computer that is not connected to a network or any other computer. For example, a stand-alone personal computer.

Logon banner: The initial message presented to a user when he or she makes connection with a computer.

Logon script: A set of stored commands that can log a user onto a computer automatically.

Master copies of software: Copies of software that are retained in an archive and that are not used for normal business activities.

Multi-user computer system: Any computer that can support more than one user simultaneously.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password reset: The assignment of a temporary password when a user forgets or loses his or her password.

Password-based access control: Software that relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user ID: A user ID that has been granted the ability to perform special activities, such as shut down a multi-user system.

Router: A device that interconnects networks using different layers of the Open Systems Interconnection (OSI) Reference Model.

Screen blanker or screen saver: A computer program that automatically blanks the screen of a computer monitor or screen after a certain period of inactivity.

Secret information: Particularly sensitive information, the disclosure of which is expected to severely damage GradLeaders USA, LLC. or its business affiliates.

Security patch: A software program used to remedy a security or other problem, commonly applied to operating systems, database management systems, and other systems software.

Sensitive information: Any information, the disclosure of which could damage GradLeaders USA, LLC. or its business associates. Shared password: A password known by or used by more than one individual.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges permitting the involved user or process to perform activities that are not normally granted to other users.

Suspending a user ID: The process of revoking the privileges associated with a user ID.

System administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

Terminal function keys: Special keys on a keyboard that can be defined to perform certain activities such as save a file.

User IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to GradLeaders USA, LLC. or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.

Appendix A – Expedient

Overview—GradLeaders USA, LLC contracts with Expedient located in Dublin, Ohio for its entire production network data center facilities. The following pages contain Expedient's Customer manual including facility descriptions, security policies and compliance documentation.

Appendix B - Agreement To Comply With Information Security Policies

A signed paper copy of this form must be submitted with all requests for authorization of a new user ID, authorization of a change in privileges associated with an existing user ID, or periodic reauthorization of an existing user ID. GradLeaders USA, LLC. management will not accept modifications to the terms and conditions of this agreement.

_____

User's Printed Name

_____

User's Department

I, the user, agree to take all reasonable precautions to assure that GradLeaders USA, LLC. internal information, or information that has been entrusted to GradLeaders USA, LLC. by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with GradLeaders USA, LLC., I agree to return to GradLeaders USA, LLC. all information to which I have had access as a result of my position with GradLeaders USA, LLC. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal GradLeaders USA, LLC. manager who is the designated information owner.

I have access to a copy of the GradLeaders USA, LLC. Information Security Policies Manual, I have read and understand the information contained in the manual, and I understand how it impacts my job. As a condition of continued employment at GradLeaders USA, LLC., I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from GradLeaders USA, LLC., and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the GradLeaders USA, LLC. Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the director of the Information Security Department.

_____

User's Signature

Appendix C – Non Disclosure Agreement

MUTUAL CONFIDENTIALITY AGREEMENT

AGREEMENT made by and between _____, a corporation with offices at _____, and GradLeaders USA, LLC a corporation with offices at 5980A Wilcox Place, Dublin, Ohio 43016 (each a "party", and collectively, the "parties").

WHEREAS, the parties are engaged in discussions regarding a potential business relationship or transaction, pursuant to which each party may have access to certain confidential and proprietary information of the other; and

WHEREAS, as a condition to being furnished with such confidential and proprietary information, each party has agreed to undertake the obligations contained in this Agreement.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby covenant and agree as follows:

1. Definition of "Confidential Information". The term "Confidential Information," as used herein, shall mean any and all information relating to the business or operations of either party hereto not generally known by others, including, but not limited to, information relating to a party's finances, organizational structure, business plan and strategies, sales, profitability, sales and marketing strategies, trade secrets, formulae, computer programs and data, agreements, customers, sources of supply and business relationships. Confidential Information shall also include comparable information that a party may receive or has received belonging to others who do business with such party. All information relating to a party's business shall be deemed to be and should be treated as Confidential Information subject to the provisions of this Agree¬ment unless clearly marked otherwise or unless (i) it was generally known to the public prior to disclosure to the other party; (ii) it becomes generally known to the public through no wrongful act or failure to act by the other party; (iii) it is disclosed to the other party by a source other than such party, which disclosure is not in breach or violation of any law or any obligation to such party or any other person or entity; or (iv) it was independently developed by the other party without any use of Confidential Information.

2. Restrictions on Disclosure and Use of Confidential Information. Each party agrees that it shall not, without the express written consent of the other, directly or indirectly give, sell, transfer, display, disclose, in any way communicate or divulge to, or (except as expressly permitted in this Agreement) use for its own benefit or the benefit of any other person or entity, any Confidential Information of the other party. Each party shall utilize any Confidential Information of the other learned of or acquired by it solely for the purpose of assessing the viability of the proposed business relationship or transaction between the parties and for no other purpose whatsoever. Each party shall take such security measures with respect to the Confidential Information of the other as are reasonably necessary to preserve the confidentiality thereof, and shall provide its employees, agents and advisors with access to Confidential Information of the other party only on a "need to know" basis. Each party shall take appropriate actions (by instruction, agreement or otherwise) with those employees, agents or advisors who are permitted access to Confidential Information of the other

party to assure their compliance with the terms and conditions hereof, and shall be liable for any breach of this Agreement by any such employee, agent or advisor.

3. Confidentiality of Discussions. Each party agrees that it shall not, without the prior written consent of the other, disclose to any person or entity either (i) the fact that discussions or negotiations are taking place concerning a possible business relationship or transaction between the parties, or (ii) any of the terms, conditions or other facts with respect to any such possible arrangement, including, without limitation, the status of negotiations with respect thereto.

4. Return of Tangible Materials. Each party hereby acknowledges that all written and other tangible materials containing or reflecting any Confidential Information of the other party or relating in any way to the business of the other party, whether furnished by the other party or prepared, compiled, developed or otherwise acquired by such party during the course of its business relationship with the other party (collectively, "Tangible Materials"), are and shall be and remain the sole property of such other party. Each party shall, at any time upon request of the other, and in any event promptly upon termination of its business relationship with the other party, return all Tangible Materials of the other party to such other party, together with all copies and reproductions thereof, and an authorized officer of such party shall certify in writing to the other party that all such Tangible Materials have been so returned.

5. Acknowledgment. Each party understands and acknowledges that neither the other party nor any of its representatives or advisors has made or makes any representation or warranty as to the accuracy or completeness of any Confidential Information or other information provided hereunder, and agrees that neither the disclosing party nor any of its representatives or advisors shall have any liability as a result of the other party's use of such information.

6. Protective Orders. In the event that either party is requested or required by a court, by governmental action or otherwise in con¬nection with legal proceedings (by oral question, interrogatories, requests for information or documents, subpoena, civil investiga¬tive demand or similar process) to disclose any Confidential Information of the other, such party agrees to promptly notify the other party in writing of such request or requirement so that the other party may seek a protective order or, in its discretion, waive compliance with the provisions of this Agreement.

7. Remedies. Each party hereby acknowledges that the remedy at law for breach or threat of breach of this Agreement is inadequate, and that the other party shall have the right to injunctive relief in the event of any such breach or threatened breach, in addition to any other remedy available to it. The existence of any claim or cause of action of any nature or description which either party may have against the other party or any agent, employee or advisor of the other party, whether predicated upon this Agreement or otherwise, shall not constitute a defense to the enforcement of the other party of the covenants herein set forth, but shall be litigated separately.

8. Severability. If any provisions of this Agreement shall be invalid or unenforceable to any extent or in any application, then the remainder of the Agreement and of such term and condi¬tion, except to such extent or in such application, shall not be affected thereby, and each and every term and condition of this Agreement shall be valid and enforced to the fullest extent and in the broadest application permitted by law.

9. Waiver. No delay or omission by either party hereto in exercising any right under this Agreement shall operate as a waiver of that right or of any other right. A waiver or consent given by a party on any one occasion shall be effective only in that instance and shall not be construed as a bar to or waiver of any right on any other occasion.

10. Construction and Interpretation. This Agreement, and all questions arising in connection herewith, shall be governed by and construed in accordance with the laws of the State of Ohio. Each party hereby submits to the jurisdiction of the courts of the State of Ohio and the federal courts of the United States of America located in such state for purposes of any action relating to the interpretation or enforcement of the provisions of this Agreement, and agrees that any legal proceedings arising under or pursuant to this Agreement shall be conducted in such state.

11. Headings. The paragraph headings contained herein are for convenience and reference only, and shall be given no effect in the interpretation of any of the provisions of this Agreement.

EXECUTED under seal as of this _____ day of _____, 2016.

_____	GradLeaders USA, LLC
By:_____	By: _____
Signature of Authorized Officer	*Signature of Authorized Officer*
_____	_____
Printed Name and Title	*Printed Name and Title*