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

Use Of Encryption Programs—Workers are reminded that [illegible] . 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 [illegible] . 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. [illegible] . 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, [illegible] . may employ content monitoring systems, message logging systems, and other electronic system management tools. By making use of [illegible] . systems, users consent to permit all information they store on [illegible] . systems to be divulged to law enforcement at the discretion of [illegible] . 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 [illegible] . 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 [illegible] . 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*