Deluxe Corporation

User's Information Security Handbook

Last Revised: April 26, 2013

Date	Version	Section(s)	Summary of Change or Action	Editor
03/15/2013		Page 4, 8	Added webcam language, 'the presence and use of' in 5th bullet on page 4; addition of webcam sentence in 6th bullet on page 8	Jeri Smith
03/18/2013		Page 4	Added wireless language 'with Mobile Devices that have not been approved by Deluxe,' in 6th bullet. Deleted 'Deluxe-approved' in 4th sentence.	Jeri Smith
03/19/2013		Page 4	Revision to add Sharon's language to wireless	Sharon Rowe
03/29/2013		Page 4	Final wireless language per Sharon and new term, Removal Media, is added	Sharon Rowe/Terry Fors (SH approved these changes)
04/04/2013		Intro, pages 4, 7, 9	'Removal Media' added to intro (pg. i,); updated Wireless language, page 4; 'Removal Media' added twice on page 7; in Personal Hardware and Software section, page 9 added, 'Mobile Devices and Removal Media' and on page 9, added example in the 5th bullet (SR has not approved yet)	Terry Fors
04/08/2013		Intro, pages 4, 7, 9	SR made changes to the wireless paragraph, then it, as well as all the other changes, were approved.	Jeri Smith
04/26/2013		Page 9	Updates to the *Personal Hardware and Software* section—specifically, bullet 4	Jeri Smith

Introduction

The purpose of this Handbook is to describe requirements for employees or Third Parties (Users) in their use of Information Technology (IT) resources owned or managed by, or on behalf of, Deluxe Corporation or its affiliates (Deluxe or the Company). This new 2013 version has been revised to include Payment Card Industry (PCI) requirements and new Mobile Device, Removal Media and password rules.

The responsibilities described in this Handbook implement the Deluxe Policies, Standards, Procedures and Guidelines (PSPGs) on the protection of information and information resources. Effective systems' security is a team effort involving the participation and ongoing support of employees and other individuals who use IT Deluxe resources.

Users of Deluxe IT resources shall be informed of the Deluxe security requirements and conduct their activities accordingly. Inappropriate use exposes Deluxe and its clients to risks, including virus attacks, compromise of network systems and services, and damage to reputation.

Contact Enterprise Information Risk Management (EIRM) for assistance or additional information regarding this Handbook, as referenced in the Contact Information on page 1.

Table of Contents

Contact Information 1
Accountability 1
User IDs 2
Passwords 2
Access Credentials 3
Incident, Theft, or Loss Response 3
No Expectation of Privacy 3
Intellectual Property 3
Acceptable Use of Deluxe Resources 4
Insertion of Computer-Related Contact Numbers in Directories 4
Modems on Workstations Connected to Internal Networks 5
Dial-Up Connections Require Authentication 5
Remote Access/Remote Control 5
Computer Virus Control 5
Internet Usage 6
Mobile Computing and Teleworking 6
Mobile Computing and Teleworking (continued) 6
Mobile Devices 7
Email 8
Housekeeping 8
Personal Hardware and Software 9
Confidentiality 10
Glossary 11

Contact Information

Offices and Sources referenced in the Handbook

Contact	Phone/Email	Situation
Deluxe Support Center (Shoreview campus)	651-483-7605 (Shoreview) 527605 (6-digit) 1-800-328-9500 (out of area)	• Access Control support • Incident Reporting • Theft of or loss of equipment
Compliance Hotline	800-231-1757	• Legal or ethical violations
Manager or HR	n/a	• Access request initiation • Personnel issues • Initiate exception requests
EIRM	EIRM_LEADERS@deluxe.com	• Exceptions

Accountability

- Users shall be accountable for their actions in the protection of Deluxe and Deluxe client data and Information.
- Personal use shall not interfere with normal business activities, shall not involve solicitation, shall not be associated with for-profit-outside-of-business activity, and shall not expose Deluxe to embarrassment or potential legal action.
- Users shall be accountable for activities on Deluxe Information Technology resources accessed via their assigned User Identification (ID) and secret passwords. Users shall not use User ID or passwords of others to gain access to Deluxe Information Technology resources.
- Users shall abide by Deluxe requirements pertaining to Information Security, Confidentiality, and Privacy when handling Deluxe or client Information.
- Violations of Information system security requirements shall be subject to discipline that Deluxe deems appropriate to the circumstances, up to and including immediate dismissal.
- IT Security shall be notified if a security device (e.g., an authentication token, PIN, password, digital certificate, etc.) is lost or compromised. In such an Event, contact the Support Center to establish corrective actions (e.g., reset passwords, lock PINS, disable token, report a loss or theft, etc.). For additional detail, see *User IDs, Passwords,* and *Access Credentials* below.
- At the time Users are relieved of their responsibilities or terminate their relationship with Deluxe, unless otherwise agreed in writing, Deluxe property shall be returned. This includes hardware, software, Sensitive Information, such as Cardholder data, library books, documentation, building keys, magnetic access cards, Deluxe credit cards, etc.

User IDs

- User IDs are unique and assigned so there is no obvious correlation between a User ID and the actual name of the involved User. Once assigned, they may not be re-used.
- User IDs shall be set up in a disabled or revoked status whenever possible, until an initial one-time password is communicated to the User. Where technically available and business applicable, User IDs shall automatically have the associated privileges suspended or revoked after sixty (60) days of inactivity and shall be deleted after a thirteen (13)-month period of inactivity. Subject to Management approval, a User ID may be deleted at an earlier date.
- Except to meet the security needs of Deluxe, Users shall not log on or use another person's User ID to perform functionality without written permission from EIRM. If there is a need to read another's mail while a User is absent, message forwarding and other facilities may be used. In other areas where similar functionality to another User is required, a manager will submit a request to EIRM.
- When system access controls initiate a lockout (e.g., the User fails to provide the correct password after three [3] incorrect logon attempts), then the User ID or password shall be revoked or locked out. When passwords are revoked, the User shall request a password reset and confirm their identity.

Passwords

- Users shall protect their passwords and access credentials.
- Passwords believed to be compromised (e.g., known by anyone other than the authorized User) shall be changed immediately. Passwords may be shared with system maintainers but shall be changed after maintenance is complete.
- Users may use the same password on internal systems, network devices, or applications, but shall not use their internal password for external systems, such as for accounts on an external web site, because these external web sites may not protect passwords in an acceptable manner.
- Unless otherwise required, passwords shall be at least seven (7) characters in length and have at least three (3) of the following attributes: a letter, number, uppercase letter, and special character.
- Users shall not construct passwords that are identical or substantially similar to passwords that they had previously employed. Passwords shall not be repeated.
- Users shall change their passwords at a minimum of every sixty (60) days.
- Passwords shall not be documented in an unsecured area. In instances where multiple levels of security exist, PINs or passwords should not be stored in the same location.
- When system access controls initiate a lockout (e.g., the User fails to provide the correct password after three [3] incorrect logon attempts), then the User ID or password shall be revoked or locked out. When passwords are revoked, the User shall request a password reset and confirm their identity.
- Administrators or other super Users who have two (2) accounts on the same system shall use passwords that are unique to each account. Administrative or system accounts shall be, at minimum, twelve (12) characters and have at least three (3) of the following attributes: a letter, number, uppercase letter, and special character.
- Default passwords for system-generated accounts (accounts created automatically during system setup) shall be changed by their first administrator or first User to prevent unauthorized use of the accounts.

Access Credentials	• Users shall protect their passwords and access credentials. • Individuals who need access shall have their immediate manager or their Relationship Manager send approval to EIRM prior to being granted a User ID or given privileges to use Deluxe computers systems. • Credentials (e.g., the combination of User IDs, passwords, and/or access tokens) that allow access to Deluxe or client Information, data, or systems are the property of Deluxe or its clients and shall only be used in accordance with Deluxe Policy. • Users shall protect passwords, badges, and other access credentials to which they have access. Each User is responsible for protecting the access credentials assigned to him or her and shall not share them with anyone else. If physical access credentials (e.g., security tokens, proximity cards, etc.) are lost or stolen, Users shall report this to their supervisor immediately to avoid unauthorized access or misuse. • When system access controls initiate a lockout, (e.g., the User fails to provide the correct password after three [3] incorrect logon attempts), then the User ID or password shall be revoked or locked out. When passwords are revoked, the User shall request a password reset and confirm his/her identity.
Incident, Theft, or Loss Response	• Users shall contact Management and call the Deluxe Support Center at 1-800-328-9500 if they suspect a Security Policy violation, system intrusion, virus, or other malicious software on a Deluxe system. Users shall also report a loss or theft of Deluxe property or Information to the Deluxe Support Center and their immediate supervisor.
No Expectation of Privacy	• Users shall have no expectation of privacy when using Deluxe Information Technology resources (including computers). Accordingly, Users shall not have an expectation of privacy in anything that they create, place on, store, send, or receive on Deluxe-owned Information Technology resources. • Users shall respect the privacy of others when handling their personal Information and shall take precautions to protect Sensitive Information, such as Cardholder data, transmitted or received via computer networks and other communication devices including, but not limited to, faxes and Mobile Devices.
Intellectual Property	• Intellectual property shall be protected. • Users shall not violate intellectual property laws (this includes copyrights, patents, trademarks, trade secrets, and/or proprietary works) and shall abide by the terms and conditions associated with the use of the intellectual property. • Violations include, but are not limited to, illegal copying, distributing, downloading, and/or uploading Information from the Internet (or electronic sources). • Examples of commonly copyrighted items are audio materials, movies, videos, software, video games, pictures, and images. Applicable software copyright and licensing laws shall be followed.

Acceptable Use of Deluxe Resources	• Deluxe IT resources shall be used appropriately in a professional manner. • Users shall not use the Internet to stalk others, post, transmit, request, or originate unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or communication where the message, or its transmission or distribution, would constitute a criminal offense, give rise to civil liability, or otherwise violate applicable laws. • Users shall not access or attempt to gain access to computer accounts to which they are not authorized. Users shall not intercept or attempt to intercept data transmissions for which they not authorized. • Users shall not use Deluxe IT resources for financial gain or commercial use; nor shall the resources be used for illegal activity. Deluxe IT resources shall be used for business purposes only. Limited personal use of Deluxe IT resources is allowable on a case-by-case basis as determined by the User's Manager or Relationship Manager, but shall not interfere with the User's work responsibilities. • Users shall access the Internet from Deluxe-owned or approved computer hardware and software primarily for conducting and promoting Deluxe business. When accessing the Deluxe intranet from a remote source connected to the Deluxe internal network, connections shall be through the Deluxe network-managed firewall. Users shall be authenticated by a User ID and password. Other direct connections to the internal Deluxe network by external sources shall first be approved by EIRM. • The presence and use of Deluxe-owned photographic, video, audio or other recording equipment (such as digital cameras, webcams and laptops with webcams) shall be allowed only with management approval in ways that do not place Sensitive information at risk, affect the privacy of employees, contractors or third party users, or disrupt business activities. Webcams that are built into Deluxe-owned laptops shall be disabled by default. • When using Deluxe-approved Mobile Devices, Users shall only connect to Deluxe-approved wireless networks when in a Deluxe facility. When working on behalf of Deluxe with Mobile Devices that have not been approved by Deluxe, Users shall only connect to Deluxe-approved wireless networks when in a Deluxe facility. The use of Deluxe-approved wireless networks is for business purposes only. When a Mobile Device is connected to the wired Deluxe network, wireless access shall be disabled. When not within Deluxe facilities, Users shall not connect Deluxe-owned Mobile Devices to wired or wireless networks without permission of the network provider. • Users shall not copy or remove Deluxe-owned software for personal use.
Insertion of Computer-Related Contact Numbers in Directories	• Information regarding access to Deluxe computer and communication systems, such as dial-up modem phone numbers, is Confidential. • This Information shall not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or made available to Third Parties without the written permission of EIRM.

Modems on Workstations Connected to Internal Networks	• If dial-out capabilities are required for business purposes, connection shall be through a secured communications server. Modems will be hardware configurable. • If a computer contains Deluxe Sensitive Information, such as Cardholder data, or is active on the Deluxe network, it cannot be connected via dial-up to an external Internet Service Provider (ISP) without an approved and managed firewall. • Analog lines at the workstation shall be limited and installed on a case-by-case basis. • Requests for exceptions to this Policy shall be submitted to EIRM through Management and include a description of the situation or circumstance (business, technical, environmental or financial) that results in the need for an exception.
Dial-Up Connections Require Authentication	• Dial-up lines connected to Deluxe internal networks or computer systems shall pass through an additional access control point for authentication before Users can reach a logon banner.
Remote Access/Remote Control	• Remote Access and Remote Control are granted on a case-by-case basis. Use of technology for Remote Access/Remote Control shall be authorized by EIRM. Remote access and remote control shall be carried out over secure computers, unless permission is otherwise granted by EIRM.
Computer Virus Control	• Users shall maintain the security of Deluxe IT resources and protect them from unauthorized access and malicious software, such as viruses, Trojan horses, worms, and spyware. Users should be cautious of file attachments they did not request. Users shall take appropriate precautions when working with such attachments. • Users shall not turn off anti-virus software or circumvent its operation. • Computer viruses shall be eradicated as soon as possible to limit damage to computers and data. Users are expected to report a computer virus to the Deluxe Support Center by phone immediately. • If a report of a known infestation is not promptly made, and if an investigation reveals a User was aware of the infestation, the User may be subject to disciplinary action, including termination of employment or Third Party engagement. Virus protection software shall not be removed from or turned off on a personal computer by the end User and shall have the most current updates.

Internet Usage	• Internet technologies shall be used primarily as a business tool and shall be used in accordance with existing Deluxe EIRM Policies, Standards and Procedures (PSPs) in effect for Deluxe or Deluxe subsidiaries. Prohibited content includes, but is not limited to, sexually explicit and/or offensive content, chain letters, illegal activities, etc. • Internet technologies include, but are not limited to, e-mail over the Internet, browsing the Internet, participating in Internet news groups or forums, retrieving programs or applications from sites on the Internet, or placing Information for viewing on a web site. • Users who discover they have connected with a web site that should be restricted (potentially offensive materials that might be construed as creating a "hostile working environment" such as, but not limited to, sexually explicit, racist, violence, and gambling) should notify EIRM of the web site name and immediately exit the site. • Deluxe may monitor, read, store, and copy Internet/intranet communications. Users do not have a right of privacy in their use of Deluxe-provided Internet/Intranet technologies. • Deluxe limits downloading software from the Internet to an as-needed basis because of licensing requirements and the significant Risk of infecting Deluxe systems with a virus/Trojan, potential back-doors and the unreliability of such downloaded software. Exceptions to these Policies will be handled on a case-by-case basis by EIRM.
Mobile Computing and Teleworking	• Anti-virus software and system patches: Users who remotely access Deluxe Information and Information Technology (IT) resources shall, as a condition of access, ensure that the devices they use to connect are protected from malicious code and that patches for their operating system and applications are installed. • Virtual Private Network (VPN)/Encrypted Connections: Devices that are authorized to connect to Deluxe Information and IT resources via a digital subscriber line (DSL), cable modem, or other Internet access medium service shall do so via the appropriate VPN or web-encrypted connection, such as secure sockets layer (SSL). • Deluxe Rights to Verify Configurations: Deluxe retains the right to verify that anti-virus software and operating system security patches are up to date prior to or during the remote access connection. Devices that are a Threat to the Deluxe network shall be disconnected and denied future access until their compliance is verified. • Deluxe-owned laptops shall be secured when they are not under the personal protection of their assigned User. Deluxe laptops that contain Deluxe Sensitive Information (this includes client Information, such as Cardholder data) shall accompany the traveler and shall not be placed into unattended checked baggage.
Mobile Computing and Teleworking (continued)	• Deluxe Sensitive Information, such as Cardholder data, on Deluxe-owned laptops shall be encrypted when the laptop is powered down. • Sensitive Information, such as Cardholder data, shall not be installed on personal laptops or other portable devices. • If an exception is approved, Deluxe Sensitive Information, such as Cardholder data, on personal laptops used for Deluxe business shall be encrypted when the laptop is powered down.

Mobile Devices

- Users shall adhere to Deluxe-required security measures while using a Mobile Device or Removal Media that connects or attempts to connect to Deluxe's internal networks or related technology resources. Failure to do so shall result in immediate suspension of network access privileges, so as to protect Deluxe infrastructure. Such security measures include, but are not limited to, physical security measures, whether or not the Mobile Device or Removal Media are actually in use, and Users shall use secure remote access and authentication Procedures.
- Users shall not disclose their Deluxe-related passwords to anyone.
- Users may use a privately owned Mobile Device for business purposes subject to these requirements. Access to, or removal of, Information on Deluxe's networks or technology-based resources is prohibited unless approved by Deluxe EIRM. The Deluxe IT department shall not technically support Third Party Mobile Device technology. Deluxe shall not reimburse Users for business use of a privately owned Mobile Device.
- Users shall protect Mobile Devices or Removal Media from loss of equipment and disclosure of Sensitive Information belonging to or maintained by Deluxe.
- Users shall immediately report to their manager and Deluxe EIRM department each incident or suspected incident of unauthorized access to and/or disclosure of Deluxe resources, databases, networks, etc.
- Users should have no expectation of privacy when using a Mobile Device to connect to the Deluxe network. Access and/or connection to Deluxe networks may be monitored, and Deluxe may turn off or deny access to the Deluxe network without notice.
- Mobile Device users shall use their phones and cameras in ways that do not place Sensitive Information at Risk, affect the privacy of employees, contractors or third-party users, or disrupt business activities.
- Deluxe may reconfigure or delete the contents of a Mobile Device without notice. At the end of a User's tenure with Deluxe, Information on the Mobile Device shall be deleted, and the Mobile Device shall be returned to 'factory default' status.

Email/ Collaboration Technologies

- Deluxe mailboxes shall be scanned for viruses and malware. The anti-virus scanning engines and pattern files shall be updated automatically as they are released by the vendor. Mailbox restrictions are set, based on Job Codes.
- The Deluxe mail system shall be used primarily for business purposes. Messages received by electronic mail are Deluxe records. Personal use shall be kept to a minimum. Workers shall be responsible for exercising good judgment regarding the reasonableness of personal use. If there is uncertainty, Users should consult their manager. Excessive use shall be subject to discipline.
- Inbound electronic mail messages shall be automatically scanned for certain keywords (which might indicate the presence of inappropriate data, such as sexist, racist or bigoted comments, etc.) and file types (which might indicate unauthorized graphics, such as pornography).
- Mail received containing possible inappropriate data, or unauthorized graphics shall be quarantined. Recipients (e-mail Users) may, from time-to-time, be notified of a quarantined message. It is the recipient's responsibility to contact EIRM with a legitimate reason to release a quarantined message. Quarantined messages shall be automatically deleted at a set interval. EIRM reserves the right to review the message before releasing it to the recipient.
- E-mail is not considered private. While Deluxe's network administration wants to provide a degree of privacy, Users should be aware that the data they create or receive on Company systems remains the property of Deluxe. Because of the need to protect Deluxe's network, Management will not guarantee the Confidentiality of Information stored on network devices belonging to or controlled by Deluxe.
- Deluxe reserves the right to monitor, record, and access e-mail sent or received by Deluxe e-mail accounts and data, Information, and files stored on Deluxe systems and equipment. The use of only Deluxe-approved collaboration software, tools and utilities shall be allowed including, but not limited to, video conferencing and messaging technologies.
- Users shall not send unsolicited commercial advertising or product advertisement e-mail for reasons other than authorized Deluxe business.
- Users shall not send types of mass mailing that does not pertain to Deluxe business or results in network spamming.
- Users shall not use automatic e-mail forwarding.
- Users shall practice e-mail etiquette.

Housekeeping

- In observance of the Deluxe ESS&H Procedure, *Security Best Practice for After Hours Clean Desk*, Users shall keep Sensitive Information, such as Cardholder data, out of plain sight (preferably in a locked drawer or cabinet) unless in use, and shall not leave Sensitive Information or Cardholder data displayed on computer screens when it is not needed.
- Users shall lock their computer, via the Crtl+Alt+Del function, or log out when leaving it unattended.
- Password-protected screensavers for laptop and workstations shall be set to activate after a period of inactivity.

Personal Hardware and Software

- The use of personal resources to conduct Deluxe business shall be specifically authorized by Deluxe Management and EIRM on a case-by-case basis. Group exceptions shall not be permitted.
- Virus protection shall be installed and updated on personally owned Information resources that connect to the Deluxe network or that process, transmit, or store Deluxe Information.
- Deluxe shall not be responsible for the repair, maintenance, or upkeep of personal IT resources used for Deluxe business.
- Users permitted to use their personal IT resources for Deluxe business shall be aware of and comply with the additional protection, dissemination, retention, and/or destruction responsibilities that come with having Sensitive records, protected records or Cardholder data on their personal computers, Mobile Devices and Removal Media (e.g., at home and during travel) described in this Handbook. The responsibility to protect Deluxe Information remains the same on personal resources as it is on Deluxe resources.
- Users shall not install personal software on Deluxe IT resources without approval by the User's Manager and EIRM. Personal software approved for installation shall be properly licensed and approved by the User's Manager and EIRM.

Confidentiality

- Users shall be accountable for protecting Deluxe Information Assets, during and after their relationship with Deluxe. Users are subject to Confidentiality requirements with respect to Deluxe and client Information as a condition of employment or being permitted to work on behalf of Deluxe.
- If requested, certain Deluxe employees shall sign Confidentiality/Non-Disclosure Agreements with Deluxe clients to further describe use of client data and responsibilities for its protection.
- Users shall not disclose Sensitive Information, including client Information, such as Cardholder data, or other Deluxe Information entrusted to their safekeeping, to anyone not authorized to receive such Information.
- Users shall properly store Sensitive, critical data and Cardholder data on a network resource that is backed-up regularly or is otherwise adequately protected by encryption.
- Users shall protect mobile resources (e.g., Removal Media and Mobile Devices including, but not limited to, laptops, smart phones and tablets), from unauthorized access at work, at home, and while traveling.
- Portable Media devices (e.g., thumb drives, flash drives, jump drives, etc.) shall use approved encryption mechanisms (e.g., AES 256-bit encryption) to protect data stored on those devices.
- Printers shall not be left unattended when Sensitive Information, such as Cardholder data, is being printed or will soon be printed. The persons attending the printer shall be authorized to examine the Information being printed. Unattended printing shall be permitted if the area surrounding the printer is physically protected to limit access.
- Users shall follow Deluxe requirements for the security of Sensitive Information, such as Cardholder data, which is stored or transmitted outside of Deluxe's control. For instance, when technically possible, Users shall encrypt Sensitive Information, such as Cardholder data, stored on Removable Media or Mobile Devices in their control or when transmitting such Information external to the local network, such as via e-mail. Contact IT Security for specific requirements.

Glossary

Term	Definition
Asset	Anything that has value to Deluxe. For the purpose of this manual, "Asset" will be equivalent to "IT Asset," which includes information; purchased, leased or licensed hardware, software, or device; and related contract services, many of which may involve Third Parties to whom there are financial and legal obligations, as well as potential liabilities. RIA includes facilities, personnel, processes and information.
Cardholder data	In this Handbook, Cardholder data refers to the Payment Card Industry (PCI).
Confidential Information	Confidential Information is Sensitive in nature, or otherwise restricted by regulation or contractual provisions, and distribution is limited to those with a legitimate need for access. Unauthorized disclosure of this Information may be in violation of legal requirements, regulatory requirements or commitments made to customers; reduce the value of the Information; or cause significant harm to Deluxe or affected Third Parties.
Event	A measurable or identifiable occurrence
Guideline	A particular way of accomplishing something that is less prescriptive than a Procedure
Information	Data that has value
Information Security	1) As an assignment, Enterprise Information Risk Management at Deluxe; 2) As a function, protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction
IT	Information Technology
Media	1) Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs); 2) Material used for storage of Information. Includes paper, magnetic disks, tapes, and optical disks.
Mobile Device	Electronics that have self-contained processing units, contain wireless telecommunications and multi-media capabilities, and are easily transportable. The definition includes, but is not limited to, Devices such as smart phones, tablets laptops and notebooks.
Procedure	Defines the process or system-specific instructions for implementing or performing acts in accordance with the Policies and Standards
PSPG	Policies, Standards, Procedures or Guidelines
Relationship Manager	The Deluxe employee responsible for a Third Party relationship.
Removal Media	Storage devices that can be removed from a computer while the system is running. Removal Media are designed to be read to or written to by removable readers, writers or drives, and refers to removal readers, writers or drives, and refers to removable storage devices when they are used to transport or store data. The definition includes, but is not limited to, USB drives, thumb drives, iPads, iPods, tablets, digital cameras and smart phones.
Risk	The level of impact on Deluxe operations (including mission, functions, image or reputation), Deluxe Assets, individuals, other organizations, or the nation resulting from the operation or use of an Information system, given the potential impact of a Threat and the likelihood of that Threat occurring: • Inherent Risks are pre-existing Risks that are fundamental characteristics of the Asset. • Incremental Risks are introduced by changes in the Asset. • Residual Risks are Risks that remain after controls are applied.
Security Policy	Security Policy refers to the Deluxe *Information Security Policy Manual*. It is a high-level statement of requirements Deluxe's management personnel communicates to Users.
Sensitive	Information classified as Restricted, Confidential, Internal Use Only and Non-Public.
Standard	A collection of system-specific or procedural-specific requirements that are expected to be met by Deluxe Users.
Third Party	Service Provider, vendor, contractor, consultancy, or business partner providing services to Deluxe
Threat	The potential for a Threat source to intentionally exploit or accidentally trigger a specific vulnerability. Threats include human errors, purposeful attacks and environmental disruptions.
User	An employee, contractor or Third Party who works with Deluxe systems or Information.