Information Security

Protecting our corporate, customer, and employee information is an important part of the eBay, Inc. culture. As a new user in our environment, you are responsible for understanding and applying the Information Security Policies and standards which are relevant to your role.

Attached are the eBay, Inc. governing polices and some key standards which apply to all users of our environment. Please take a moment to familiarize yourself with these documents. Once you have started, be sure to visit the Information Security sites on the internal web to review the more specific standards which apply to your role and environment.

Thank you for doing your part to keep eBay secure!

The Information Security Team

Information Security Policy Acknowledgement

All eBay employees must review eBay, Inc.'s Information Security Policy.

Please sign and date this document, acknowledging that you have read and understand the information contained in this packet.

"I have read and understood all of the security policies referenced in and attached to this document. Specifically:

- Information Security Policy
- Acceptable Use Policy
- Information Classification Standard

Print Name: _____

Signature: _____

Date: _____

Please return this completed Acknowledgement Form with your other New Hire documents.

Information Security

INFORMATION SECURITY POLICY

INTRODUCTION

The purpose of this policy is to limit the risk to eBay Inc. (“eBay”*) information resources through the management of a comprehensive information security program.

SECURITY MANAGEMENT POLICY

Executive Management endorses the mission, charter, authority and structure of Information Security. The Company's Executive Management has charged Information Security with the responsibility for developing, maintaining and communicating a comprehensive information security program to protect the confidentiality, integrity and availability of Company information resources.

RISK MANAGEMENT POLICY

Appropriate security controls must be built into the Company's information resources. This protection should be commensurate with a resource's value to the Company, as determined by the results of a formal risk assessment.

PERSONNEL MANAGEMENT POLICY

Information security controls must be implemented to ensure that personnel are appropriately screened and made aware of the Company's Information Security Policy.

PHYSICAL SECURITY POLICY

Information processing facilities and information resources must have appropriate physical access controls in place to protect them from unauthorized physical access and be safeguarded against reasonable environmental hazards.

OPERATIONS MANAGEMENT POLICY

System and application managers must be granted the minimum level of access privileges required to perform their job functions, and must adhere to formal procedures when working with all information resources. Additionally, operational duties must be segregated in accordance with a user's role and responsibilities.

SECURITY MONITORING AND RESPONSE POLICY

Critical information resources must be monitored to detect system, security and operational events. Formalized incident response and investigations procedures must exist to ensure timely response to information security incidents

COMMUNICATIONS MANAGEMENT POLICY

Exchange of information within the Company and between the Company and other organizations should be protected by adequate controls.

ACCESS CONTROL POLICY

Personnel must be positively authenticated and authorized prior to being granted access to Company information resources. Access based on an individual's role must be limited to the minimum necessary to perform their job function. Access to critical information resources must be controlled through a managed process that addresses authorizing, modifying and revoking access, and periodic review of information system privileges.

NETWORK SECURITY POLICY

Network connections within the Company and between the Company and other organizations must be protected by adequate controls.

THIRD PARTY SERIVICES POLICY

Third parties must uphold the principles of the Company’s Information Security Policy and acknowledge their responsibility through a formal written statement.

APPLICATION DEVELOPMENT POLICY

Application development activities must comply with a development methodology that incorporates appropriate information security controls into each stage.

RECOVERY AND BUSINESS CONTINUITY POLICY

The Company's critical information resources must have formally developed contingency plans that provide for the prompt and effective continuation of critical information services in the event of a disruption.

LEGAL, COMLIANCE AND REGULATORY COMPLIANCE POLICY

The Company’s Information Security Policy must comply with applicable national and local legal, regulatory, and contractual requirements.

Information Security

ACCEPTABLE USE STANDARD

INTRODUCTION

The purpose of this policy is to limit the risk to eBay Inc. (“ebay”*) information resources by establishing expectations of acceptable use of company systems and resources.

701 Standard Statements

701.1 No Expectation of Privacy

ebay may access, review, monitor, copy, block and delete Personnel’s communications for business reasons. Further, eBay may disclose personnel communications to third parties if appropriate. Thus, Personnel should not expect privacy in voicemail, email, or any communications on the network including, but not limited to, internet web sites, chat groups and newsgroups. Monitoring, disclosure and other processing of communications shall take place in accordance with applicable law.

701.2 Inspection

Any Information resource or property owned by eBay, including disks and storage media, computers, PDAs, Blackberries, phones, desks, filing cabinets, or other work areas, as well as the articles contained therein, is subject to inspection by authorized eBay personnel at any time with or without notice or consent. Inspections shall be conducted in accordance with applicable law.

701.3 Passwords

Personnel are responsible for the security of their passwords and accounts. Personnel may not share their passwords, PINs, or passphrases with anyone, including other Personnel.

701.4 Permitted Activities

Personnel agree to use eBay Inc. Information Resources for the purpose of conducting eBay Inc. business; however, eBay recognizes that, on occasion, Personnel may want to utilize eBay resources for personal use. This use is permitted on a limited basis, so long as it is in accordance with eBay’s Code of Business Conduct. Personal use is based upon acceptance of the “No Expectation of Privacy” statement above.

Personnel must follow all applicable laws and regulations when utilizing these resources. Any communications utilizing eBay Information Resources must be consistent with eBay’s Code of Business Conduct, policies, standards, values and behaviors.

701.5 Prohibited Activities

Personnel agree to refrain from conducting prohibited activities. Without limiting any other part of this standard, Personnel may not use eBay Information Resources to send, receive, store, or display communications or files, including electronic communication attachments that are illegal, disruptive, offensive to others, or contrary to our Code of Business Conduct.

Unauthorized Personnel may not gain access to other Personnel or administrative accounts.

Never view your own PayPal or eBay account or any accounts for a co-worker, friend, family member, or any other person with whom you are transacting. In the event that you or someone you know needs assistance, place a call to the appropriate customer service center.

701.6 Third Party Materials

Personnel should not redistribute or copy third party materials without their permission. Articles, photos, graphics, sound files, and other attachments are often the intellectual property of another party. Personnel should assume that anything they download from the Internet is protected by intellectual property laws, and the use or redistribution of those materials is governed by license from the content owners. Consult with the appropriate management or legal department for any questions regarding appropriate use of these materials.

701.7 Return of eBay Property

Personnel are responsible for all property, materials, or written information issued to them or in their possession or control. Upon termination of employment or contract, or immediately upon request, Personnel must return to eBay all documents (and all copies thereof) and other eBay property and materials in their possession or control in accordance with the Proprietary Information and Invention Assignment Agreements or other similar contracts between Personnel and eBay.

These include but are not limited to:

- Computer systems
- Phones
- Mobile computing devices
- Files
- Notes
- Memoranda
- Correspondence
- Lists
- Drawings
- Records
- Plans and forecasts
- Financial information
- Personnel information
- Customer and customer prospect information
- Sales and marketing information
- Product development and pricing information
- Specifications
- Computer-recorded information
- Tangible property
- Credit cards
- Entry cards
- Identification badges and keys
- Third party information

Materials of any kind which contain or embody any proprietary, confidential or restricted material of eBay, as defined in the eBay Inc. Information Classification and Handling Standard, and all reproductions thereof.

eBay may take all action deemed appropriate to recover or protect its property.

701.8 Handling of Information

All information must be handled in accordance with the eBay Inc. Information Classification and Handling standards.

701.9 Electronic Communication Usage

Personnel must exercise the utmost caution when sending any electronic communication to outside parties.

Electronic communications must adhere to the handling requirements specified in the eBay Inc. Information Classification and Handling Standard.

701.10 Blogging and Social Networking

All blogging and social networking site usage must adhere to the eBay Inc. Blogging and Social Networking Guidelines.

701.11 Electronic Communication Retention

Personnel must adhere to the Email Retention Policy managed by the Legal department.

701.12 Prohibited Electronic Communication Activities

The following activities are strictly forbidden:

- Sending unsolicited electronic communication messages, including 'junk mail' or other advertising material to individuals who did not specifically request such material (email spam).
- Sending any form of harassment via electronic communication, including, but not limited to, language or message frequency.
- Sending messages that would impede anyone's ability to utilize information resources including frequent or large messages resulting in denial of service to the recipient or other network users.
- Unauthorized use or forging of electronic communication header information.
- Soliciting electronic communications for any other electronic communication address other than the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding Spam, 'chain letters', 'Ponzi' or other pyramid schemes of any type.
- Using unsolicited electronic communications originating from within the eBay's network on behalf of, or to advertise, any service hosted by eBay or connected via eBay's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM).
- Automatically forwarding electronic communications from a work account to another electronic communication account.
- Opening any files or macros attached to an electronic communication from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then 'double delete' them by emptying the Trash (Recycle Bin).

701.13 Prohibited System and Network Activities

The following activities are strictly prohibited:

- Unauthorized copying, distribution, usage, or installation of third-party intellectual property without permission.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Appropriate management should be consulted prior to export of any material that is in question.
- Effecting security breaches or disruptions of network communication. Security breaches and disruptions include, but are not limited to, accessing data of which the person is not an intended recipient, logging into a server or account that the person is not expressly authorized to access, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning unless authorized by the appropriate information security authority.
- Circumvention of user authentication or security of any host, network or account unless authorized by the appropriate information security authority.
- Interfering with or denying service to any personnel.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means.
- Intentionally creating, using, or storing any viruses, Trojan horses, worms, time bombs, cancelbots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept, or expropriate any system, data or personal information.
- Executing unapproved Malware prevention software.
- Implementing or connecting to any eBay network via unauthorized wireless networks, equipment, or devices. The Global Service Desk has further information about approved equipment and devices.
- Creating or using unauthorized access to eBay networks, systems, or data including, but not limited to, modems and wireless devices.
- Congesting the network or interfering with the work of others, including the transmission or posting of messages that are intended or likely to result in the loss of the recipient’s work or systems.
- Using the eBay network to gain unauthorized access to third party resources.
- Downloading files from unknown or suspicious sources.
- Using media from an external source without first performing a virus scan on it.
- eBay reserves the right to disable or limit personal use (such as streaming video/media) of eBay resources via the VPN (from office or home) without any notice.

701.14 Unattended Personnel Equipment and Clear Screen

Personnel must not leave their computing device or terminal unattended without either logging-out of or locking their system.

701.15 Clean Desk

Users must not leave their workspace or meeting room unattended without clearing their desk or common areas of any Internal, Confidential or Restricted information, as defined in the Information Classification standard.

INFORMATION CLASSIFICATION STANDARD

INTRODUCTION

The purpose of this policy is to limit the risk to eBay Inc. (“ebay”*) information resources through the management of information resources.

801.1 CLASSIFICATIONS

There are four classifications of eBay Inc. information:

Public - Information that is readily available or disclosed to all parties. Public information does not need to be classified; however, copyright or trademark protections may apply.

Internal - Information that is intended for distribution to anyone within ebay but should not be disclosed outside of the company. This classification is for information that is typically accessible to anyone working at ebay to view and have access to, regardless of their job or business function.

Confidential - Information that is intended only for a limited audience within eBay Inc. or whose release would likely have an adverse financial or reputational effect on ebay, ebay employees, or ebay users and or consolidated subsidiaries. All customer and employee non-public personal information, non-public financial information, and intellectual property shall have a minimum classification of confidential. Information in this category must be limited to only those with a business need for access. (Examples include, but are not limited to: software source code, employee records such as salary, stock and benefits information, customer and employee personal contact information, customer email addresses, design diagrams, etc.)

Restricted - Highly sensitive or regulated information that is intended only for a limited audience within eBay or whose release would likely have a material adverse financial or reputational effect on eBay, eBay employees, or eBay users and or consolidated subsidiaries. All information in this category will be restricted to a limited group with authorized need to know access. (Examples include but are not limited to: credit card information, bank account information, social security numbers, date of birth, driver’s license numbers, pre-release financials, pre-acquisition information, passwords, encryption keys, etc.) Information about proposed or pending mergers and acquisitions shall be considered restricted.

801.2 HANDLING

Information must be handled according to the Information Handling Standard. (Inc-Information Security-STD-802.1.0-Information Handling)

Information must be labeled according the Information Labeling Standard (Inc-Information Security-STD-803.1.0-Information Labeling)

All information is presumed to be at least "Internal” unless otherwise classified. In all circumstances, sound business judgment must be applied and information must not be publicly released until it is confirmed to be public information by the information owner.

Users who encounter information that is improperly handled according to the information classification must consult with the owner of the information to determine the appropriate classification.

A current list of classified data fields is provided in the Classification of Elements Standard Operating Procedure. If multiple data fields with different classifications have been combined, the highest classification of information included will determine the classification of the entire set.

If a change in sensitivity of information results in reclassification to a higher level, the owner must ensure appropriate handling requirements are being met.