Non-Associate

Information Security and Acceptable Use Standards for Assignment at JM Family Enterprises, Inc. (JMFE)

Overview

JM Family Enterprises, Inc. and its subsidiaries ("JMFE") is committed to managing Information and Information Assets responsibly in order to maintain their security, confidentiality, integrity and availability, as well as to comply with applicable laws, regulations and obligations JMFE has to third parties, such as its customers and business partners.

Every time you access or use Information Assets and/or Information, you are indicating your agreement to be bound by these standards. JMFE may change these standards at any time and you are responsible for complying with these standards as they are updated or revised.

The purpose of these standards are to establish the Information Security criteria necessary to safeguard the confidentiality, integrity, and availability of JMFE Information, including establishing what constitutes acceptable use of certain JMFE Information and Information Assets.

Scope

These standards apply to the Information of JMFE. All Authorized Users are responsible for adhering to these standards.

Capitalized terms used herein are defined below under "Definitions." Specific procedural guidelines for these standards are available in the "Related Information" section.

General Provisions

- JMFE Information created by, stored by, acquired by, contained in, or processed by JMFE Information Assets is owned by JMFE wherever it exists and regardless of its location or storage medium (e.g., personally owned computing equipment, third party owned computing equipment, tablets, cell phones, voice mail).
- All JMFE Information must be protected by all Authorized Users against unauthorized disclosure, modification, compromise, or destruction.
- Protection of all JMFE Information is required regardless of whether the Information has been classified in accordance with these standards.
- JMFE Information, including Information about JMFE's activities, business plans, products, associates, and customers, must not be disclosed outside of JMFE without approval from

management who has ownership responsibility or without secured appropriate protections for that Information.

- JMFE must comply with all applicable legislative, statutory, regulatory, and contractual requirements related to Information Security.

Acceptable Use

- Only Authorized Users may use or access Information and Information Assets. If you become aware of any unauthorized use of Information or Information Assets, any weaknesses in JMFE computer security, or any other security related issue, contact the Service Desk at 1-888-739-6800 immediately. As an Authorized User, you are responsible for exercising good judgment in accordance with the Non-Associate Code of Business Conduct and other applicable policies in your use of Information and Information Assets. You are responsible for the security of Information and Information Assets under your control.

- **You have no right to or expectation of privacy when you use or access Information Assets or when you send, receive, store, or give access to Information through Information Assets**. In other words, anything that you create, send, receive, store or access (e.g., personal tax returns) by or through Information Assets is subject to inspection and monitoring and can be viewed, copied, saved, received, or otherwise used by JMFE, without prior notice. This includes any communications that you may have with your personal advisors, including lawyers, accountants, brokers, and others, even if made with your personal accounts while using JMFE's Information Assets.

- Certain confidentiality privileges apply to your communications with lawyers and other similar professionals; if you use Information Assets to conduct personal business with such professionals, you may waive or lose these rights to confidentiality as a result. Additionally, any pictures, data or other personal content and any applications (apps) you may have on your JMFE provided cell phone or mobile device can be viewed by JMFE, even if you purchased and/or installed such content or applications (apps) from your personal account, such as your personal iTunes account.

Identity and Access Management

- All Authorized Users play an important role in ensuring the confidentiality, integrity, and availability of Information and automated systems through the use of logon accounts, authentication codes, and other means of authentication.
- In order to access JMFE's network and systems, you must be assigned and use a unique logon account. You must protect your logon account.
- You should not attempt to access, modify or delete any data, documents, email correspondence, or programs for which you do not have authorization.

- Access to JMFE systems and networks is granted utilizing the Least Privilege Principle.
- System administrators are responsible for protecting the account information (i.e., logon account, passwords) entrusted to them. System owners are responsible for ensuring that access is appropriate and authorized.

Password Protection

- Passwords are required for all Authorized Users who have or are responsible for an account on any system residing at any JMFE facility, have access to the JMFE network, or store any Sensitive Information.
- All Authorized Users are responsible for creating strong passwords for the best security using the tips found in the Non-Associate Acceptable Use Procedure.
- You must protect and never share passwords, Personal Identification Numbers (PINs), Security Tokens (e.g., Smartcard), IDs or similar information or devices used for identification and/or authentication. **No one should ever request your password, including the Service Desk or support personnel.**

Encryption

- If you are sharing or transmitting Information outside of JMFE, you must take measures to protect the confidentiality and security of Information.
- Use JMFE approved encryption and other tools for sending or sharing Sensitive Information outside of JMFE's network. Contact the Service Desk at 1-888-739-6800 for assistance with transmission of Sensitive Information outside of JMFE systems.
- Before storing information on mobile devices such as USB, CD, DVD, or laptops, Authorized Users must always ensure Sensitive Information is protected. See the Non-Associate Acceptable Use Procedure for additional information.

Information Asset Management

- JMFE hardware must be protected from actions that could jeopardize the confidentiality, integrity, or availability of Information and automated systems. You should pay particular attention to your surroundings, making every effort to protect JMFE Information and Information Assets from unauthorized access:
    - At all times and especially when in public areas, Authorized Users must protect Sensitive Information from "shoulder surfing" by positioning workstation or laptop screens away from visibility.
- JMFE hardware is provided for conducting JMFE business and management approved activities. When no longer needed, hardware must be returned timely.

- Only JMFE owned or leased hardware may be used on the JMFE network. Non JMFE owned or leased hardware is permitted to connect to the JMFE network only through approved and designated gateways.

Clear Desk and Clear Screen

- Authorized Users are expected to protect Sensitive Information that they create, access and/or use, including:
  - Clear Desk: Authorized Users are required to remove Sensitive Information from their open work area anytime their work area cannot be monitored during the workday. Authorized Users are required to remove and secure Sensitive Information from their open work area before leaving at the end of the day.
  - Clear Screen: Authorized Users are required to lock their screens in any situation where they are away from their computer, including for meetings, restroom breaks, lunch and before leaving at the end of the day.
  - Offices: If an office door can be locked, the removal of Sensitive Information from the work area is not required if the office door is shut and locked.
  - File Cabinets: Cabinets containing Sensitive Information must be locked at all times when not in use.
  - Printers: Sensitive Information must not be left unattended at printers.
- Unattended work areas must be clear of Sensitive Information in any form.

Anti-Virus and Malware Protection

- Anti-Virus and Malware Protection software must be used, and must not be disabled, to protect Information from virus infection.
- You must never download, install or run programs to test the security of JMFE Information Assets or reveal or exploit weaknesses in security unless you are authorized to do so.

Network and Communications Security

- Connections to non JMFE computers and networks must be implemented in a controlled and secure manner to ensure the confidentiality, integrity, availability, and authenticity of Information transmitted between JMFE computer systems and outside networks and computers. Implementers and administrators of the network and network perimeter security technologies are responsible for adhering to key control standards.
- Connectivity to or from the JMFE network must be coordinated through Information Technology Services and approved by the JMFE Chief Information Security Officer (CISO).
- Remote access to Information Assets, wherever they reside, must be approved through multi-factor authentication and requires prior approval.

- You must not email or transfer Sensitive Information to personal email accounts or storage. By following JMFE remote access procedures in the Non-Associate Acceptable Use Procedure, all Information is securely accessible when outside of the JMFE network.

Data and Information Management

- All Authorized Users are responsible for retaining, managing, and disposing of Information and Information Assets appropriately.
- Owners of Information are responsible for assessing the need for classifying Information. The assigned classification will be used to determine an appropriate level of access control, retention, and method of destruction. Three factors generally identify Information requiring protection:
    - Sensitivity to disclosure (confidentiality)
    - Sensitivity to modification (integrity)
    - Sensitivity to destruction (availability)

Software Licensing

- Only approved licensed software may be loaded on JMFE workstations, laptops, and servers. Mobile device Authorized Users are allowed to purchase and download software from the operating system provider's application store.
- Always comply with copyrights and software licenses.

Definitions

Authorized User: Any Associate, temporary worker, consultant, contractor, vendor, agent, volunteer or other person or entity who is authorized to use Information Assets and/or to access Information related to JMFE's business under the terms and conditions of these standards.

Information: Any and all data, regardless of form (electronic or otherwise), that is created by, stored by, acquired by, contained in, or processed by, Information Assets. Information includes, but is not limited to, voicemail, e-mail, text messages, instant messages, documents, spreadsheets, and databases.

Information Assets: Any and all digital, electronic or telecommunication resources that are used in JMFE's offices, during business travel or otherwise provided by JMFE for the purpose of conducting business on behalf of JMFE. Information Assets include, but are not limited to, physical resources such as telephones, cameras, cell phones, tablets, computers, laptops, fax machines, printers, scanners, copiers, removable storage devices (e.g., USBs, CDs, DVDs, removable hard drives) and non physical resources such as company intranets, applications on JMFE's network, cloud-based networks and software, internet and JMFE network access and connectivity, phone systems, e-mail, instant messaging, accounts, voicemail, collaboration tools and JMFE social media sites.

Least Privilege Principle: The practice of limiting access by giving Authorized Users the lowest level of user rights necessary to perform their job responsibilities.

Regulated Data: Regulated data is Information which generally falls into the following categories:

- Information which is: provided by an individual to obtain a financial product or service (e.g., names, addresses, driver's license, social security and account numbers); or
- about an individual resulting from a transaction between the individual and the financial institution, including the fact of the individual's relationship with the financial institution; or
- otherwise obtained about an individual in connection with providing a financial product or service; or
- any list, description or grouping of individuals (including publicly available information about them) that is created using any of the Information described above.

- Information that can be used, either alone or in combination with other Information, to establish an individual's identity, contact or locate an individual or access an account.
- The following credit or debit card Information:
  - security related Information (Card Validation Codes/Values, complete or EMV chip track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plain text or otherwise unprotected form; or
  - full magnetic stripe on a credit or debit card; or
  - credit or debit card number plus at least one of the following:
  - cardholder name; expiration date; or service code (the three or four digit number on the magnetic stripe or EMV chip that specifies acceptance requirements and limitations of a magnetic stripe or EMV chip read transaction).
- Information that identifies an individual and relates to:
  - the physical or mental health or condition of the individual; or
  - the provision of health care to the individual; or
  - payment for the provision of health care to the individual.

Sensitive Information: Any Information, regardless of form, that:

- is distributed on a "Need to Know" basis; or
- can be accessed and used only by JMFE Associates or authorized external parties; or
- describes or is related to a confidential practice, method, process, design, or other information used by JMFE to compete with other businesses (e.g., financial statements, business plans, processes and strategies); or

- if disclosed, could be harmful to JMFE business operations, business plans, its reputation, or its Associates, or that could subject JMFE to civil or criminal penalties; or
- JMFE is obligated to keep confidential under the terms of a contract or agreement; or
- JMFE must keep confidential under a law or regulation (“Regulated Data”).