Policy

JM Family Enterprises

Last Review Date: 07/20/2022

Acceptable Use Policy

Purpose

The purpose of this policy is to establish rules and requirements for the acceptable use of Information and Information Assets associated with information and information processing at JM Family Enterprises, Inc. ("JMFE"). The rules are in place to protect JMFE Information, Information Assets, and its Authorized Users.

Scope

This policy applies to the use of Information and Information Assets that are associated with information or information processing to conduct JMFE's business or interact with internal networks and business systems. This policy applies to Authorized Users at JMFE and includes all equipment that is owned or leased by JMFE. It is the responsibility of Authorized Users to read and understand this policy and to conduct their daily duties in accordance with the terms set forth.

Policy

General Requirements

- All Authorized Users shall use appropriate safeguards to protect Information, Information Assets and networks.
- Authorized Users shall use assets for only appropriate and authorized purposes, and in accordance with published policies, standards and guidelines.
- Authorized Users shall only perform activities with their own user ID.
- Upon termination of employment, Authorized Users shall immediately cease use of all company property (e.g., Information Assets, computing resources, and intellectual property) and return all company property in their possession to the organization.
- Systems shall be used to conduct business. Personal use of systems shall not impact the performance of activities related to the Authorized User's responsibilities or violate company policies. Authorized Users shall exercise good judgement regarding the reasonableness of personal use and refer to the Code of Business Conduct for guidance.
- Proprietary information stored on electronic and computing devices owned or leased by the organization or the Authorized Users, shall remain the sole property of the organization.
- Authorized Users shall promptly report theft, damage, loss, or unauthorized disclosure of proprietary Information or Information Assets.
- Authorized individuals within the organization shall monitor equipment, systems and network traffic.
- Information Security reserves the right to audit network and systems on a periodic basis to ensure

compliance with this policy.

Clear Desk and Clear Screen

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

Privacy and Monitoring

- Authorized Users shall have no expectation of privacy for proprietary or business information they create, store, transmit, or receive via the organization's or the Authorized Users' assets (e.g., workstations, laptops, mobile devices, email and instant messaging, etc.). Authorized Users may, however, have an expectation of privacy in personal information and messages created, received, stored, and transmitted on systems in compliance with this policy unless that information creates a security risk for the company.
- The organization shall reserve the rights to:
    - Monitor for security purposes the use of organization assets by any Authorized User, including, but not limited to, websites visited, files downloaded and uploaded, and all communications sent and received by Authorized Users.
    - Monitor for security purposes organization assets with or without the Authorized User's knowledge or consent.
    - Remove from its assets any material it views as inappropriate, offensive or potentially illegal.
    - Block any unacceptable usage of organization assets.
    - Log the activities of organization assets for security purposes. These logs may record information regarding the use of organization assets, including, but not limited to, when, where, and from what device a user account has been allowed or denied access.
- Monitoring activity shall be designed to assure that the system is not used for unapproved, improper or illegal means; and to provide access to records stored on Information Assets when an associate is unavailable.

Password Security

- Authorized Users shall protect and never share passwords, Personal Identification Numbers (PINs), Security Tokens, IDs, or similar information or devices used for identification and/or authentication. No one shall ever request your password, including support personnel.
- Passwords shall be used by Authorized Users who have or are responsible for an account on any system residing at any organization facility, have access to the network, or store any Sensitive Data.
- Authorized Users shall utilize passwords compliant with the organization's specific password requirements.

Data Protection

- Authorized Users shall access, use or share proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.
- Authorized Users shall ensure that proprietary information is protected.

Email and Communication Activities

- All business-related messages on the organization's email and messaging systems shall remain the property of the organization.
- Only approved instant messaging services shall be used to conduct business.
- There shall be no expectation of personal privacy when using the organization's email and messaging systems for business-related purposes.
- Unless approved by appropriate management personnel:
    - Unsolicited email transmissions to prospects, customers and consumers shall be prohibited.
    - Authorized Users shall not make any public representation on behalf of the organization via email or instant message.
    - Automatic forwarding of internet email messages to external email systems shall be prohibited.
- The organization's email and messaging systems shall not be used to transmit material containing:
    - Derogatory remarks regarding one's race, color, sex, sexual orientation, national origin or citizenship, ancestry, religion, creed, age, disability, marital status, gender identity, veteran status or other protected statuses;
    - Sexually explicit content;
    - Offensive language;
    - Material which would negatively reflect upon the organization or threaten the safety of the workplace or contents prohibited by law or regulation.
- Authorized Users who receive messages containing such offensive material shall not forward such material to either internal or external parties, unless this forward is to notify human resources or relevant support personnel.
- Authorized Users shall not use personal email accounts for any business-related messages or

content.

Network Use

- Authorized Users shall not attempt to circumvent network security measures.
- Authorized Users shall not disable any anti-malware scanning software or the downloading of updates to such software.
- Authorized Users shall not attempt to remove malware without appropriate service personnel assistance.
- Authorized Users shall not connect unapproved devices to the organization's network or any IT resource.
- If a computer or device is suspected of being infected by a virus or malware, Authorized Users shall immediately contact the appropriate service personnel for assistance.
- If Authorized Users need to access the network from home or traveling, they shall connect remotely by using a two-factor authorization token.

Internet Use

- Internet access via the organization's network shall be revoked upon failure to follow the requirements within this document.
- While Authorized Users are on the network, personal use shall not:
  - Violate the Code of Business Conduct
  - Consume resources that could interfere with business requirements;
  - Interfere with your productivity;
- Other inappropriate internet use shall not be allowed, including but not limited to, the following:
  - Engaging in unlawful or malicious activities;
  - Accessing or downloading any pornographic, obscene or offensive material;
  - Downloading or distributing pirated software or data;
  - Downloading entertainment software or games, or playing games over the internet;
  - Uploading any software or information owned by the organization to non-organization licensed equipment or platforms without explicit authorization from appropriate management personnel;
  - Exporting software, technical information, encryption software or technology, in violation of international export control laws;
  - Use of video or audio streaming and downloading technologies that are non-business related (e.g., movies, television) and represent significant data traffic that can cause network congestion.

Physical Protection of Property

- Authorized Users shall protect company devices against unauthorized use.
- Authorized Users shall secure their PCs, laptops and workstations with a password-protected screensaver.

- Authorized Users shall take care of and safely keep assets assigned to them.
- Systems shall automatically prevent the use of external storage devices.

Software Use

- Software used on Information Assets shall be legally purchased or licensed by the organization.
- Software shall be used in accordance with the applicable licensing.
- The organization shall have the right to inspect or audit all software installed on any organization-issued computer or mobile device without warning or permission from any Authorized User.
- The organization shall have the right to request the removal of any non-authorized software found on an organization-issued computer or mobile device. However, if such non-authorized software poses a security or business-related risk, then the organization has the right to remove the non- authorized software immediately.
- Authorized Users shall not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the organization.
- Authorized Users shall not commit unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which JMFE or the end user does not have an active license is strictly prohibited.

Use of Social Media

- Organization-owned social media accounts shall only be used for business-related purposes.
- The organization shall reserve the right to monitor online activity regarding organization-owned social media accounts.
- The usage requirements in this policy apply to how Authorized Users conduct themselves online, regardless of whether they access organization-owned social media accounts at work or on personal time.

Unacceptable Use

The following activities are, in general, prohibited. Authorized Users may be exempt from these restrictions during their legitimate job responsibilities. Under no circumstances is an Authorized User authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing organization owned resources.

The list below is by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are prohibited, with no exceptions:

1. Authorized Users shall not conduct port scanning or security scanning activities unless prior notification and approvals are received from Information Security.
2. Authorized Users shall not execute any form of network monitoring which will intercept data not intended for their host unless this activity is a part of their normal job/duty.
3. Authorized Users shall not circumvent user authentication or security of any host, network or account.
4. Authorized Users shall not introduce honeypots, honeynets, or similar technology on the network.
5. Authorized Users shall not interfere with or deny service to any user (e.g., denial of service attack).
6. Authorized Users shall not use any program/script/command, or send messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
7. Authorized Users shall not provide information about, or lists of, Authorized Users to parties outside the organization.
8. Authorized Users shall not tamper, disengage, or otherwise circumvent an organization or third-party IT security controls.

Policy Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

You must read, understand, and comply with this policy. Failure to comply with this policy could result in negative impact to the organization (i.e., penalties, fees, fines) and/or disciplinary actions or contractual provisions up to and including termination of employment.

Standing Systems and Applications

Systems and applications that were implemented prior to this policy's published date are not expected to meet the requirements established within this policy. Any instances of non-compliance shall be documented and follow the risk management and risk register process.

Exceptions

Any exception to this document shall be documented, reviewed and approved as part of the Policy and Standards Exception Process. Exceptions shall be evaluated at least annually.

Superseding Policy

Over the course of time other policies may have been written and adopted by JMFE that relate to or overlap with the subject matter in this policy. This policy supersedes any and all other formal or informal policies dealing with the subject matter in this policy.