

Information Security Policy

July 09, 2019

1. INFORMATION SECURITY POLICY	3
1.1. PURPOSE	3
1.1. SCOPE	3
1.2. EXECUTIVE MANAGEMENT SUPPORT	3
1.3. INFORMATION SECURITY POLICY MANAGEMENT	3
PUBLICATION AND DISSEMINATION	4
2. RISK MANAGEMENT	4
2.1. SECURITY TESTING	4
2.2. MONITORING OF EMERGING THREATS AND VULNERABILITIES	4
2.3. VULNERABILITY MANAGEMENT PROGRAM	4
2.4. ASSET MANAGEMENT	4
DATA MANAGEMENT POLICIES	4
ACCEPTABLE USE OF COMPUTING ASSETS	4
PROPER USE OF ELECTRONIC RESOURCES	4
SOFTWARE RESTRICTIONS	5
PROPER USE OF MOBILE DEVICES	5
NETWORK ACCEPTABLE USE	5
3. OPERATIONS SECURITY	6
3.1. OPERATIONAL PROCEDURES AND RESPONSIBILITIES	6
3.2. PROTECTION AGAINST MALICIOUS SOFTWARE	6
3.3. INCIDENT RESPONSE	6
4. ACCESS CONTROL	6
4.1. BUSINESS REQUIREMENT FOR ACCESS CONTROL	6
ACCESS CONTROL POLICY	6
USER RESPONSIBILITIES	6
4.2. NETWORK SERVICES USAGE	7
4.3. EXTERNAL NETWORK CONNECTIONS, VPN, AND REMOTE ACCESS	7
4.4. SECURE LOG-ON PROCEDURES	7
5. PRIVACY POLICY	7
6. AMENDMENT/TERMINATION OF THIS POLICY	8
7. EXCEPTIONS	8
8. VIOLATIONS/ENFORCEMENT	8



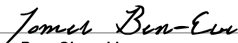

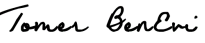
Publication Note

This policy is the property of Mursion and is exclusively for the use of Mursion employees, authorized agents, and affiliated companies. It contains Mursion confidential and proprietary information, and under no circumstances is it to be delivered or disclosed to any person not employed by Mursion, its authorized agents, or affiliated companies, without the express written authorization of an officer of Mursion.

Document Management

Revision	Release Date	Updated by	Remarks/Comments
0.1	11/28/2016	Ruchira Hasolkar	Initial Draft
0.2	12/03/2016	Arjun Nagendran	Made edits/resolved comments.
1.0	6/10/2019	Tomer Ben-Evi	SOC Review and edits

Document Approval and Acceptance

Name	Signature	Date	
Tomer Ben-Evi		6/12/2019	
Tomer BenEvi	DocuSigned by:  A1112A21C6D546F...	6/18/2020	Reviewed with no additional changes
Tomer Ben-Evi	DocuSigned by:  A1112A21C6D546F...	7/26/2021	



1. Information Security Policy

1.1. Purpose

Mursion recognizes the importance of information to the company, and the criticality of defining, establishing, and maintaining a robust information security program that protects information and computing assets. To support this objective, Mursion executive management has created this Information Security Policy, which establishes standards, controls, and guidelines for the protection of Mursion assets and customer data within the organization.

1.1. Scope

This document is Mursion's primary Information Security Policy and establishes standards for information security throughout Mursion. Several subordinate policies, including Mursion's, Incident Response Plan, Acceptable use Policy, Risk Management Policy, and others, support individual objectives of the company's Information Security Program.

All information security policies and procedures must receive management approval prior to their implementation. This policy and all its specific requirements apply to all Mursion employees, authorized agents, and affiliated companies. All such personnel or organizations are required to read, understand, and fully comply with all relevant portions of this policy.

1.2. Executive Management Support

This document has been created by the Information Security Department in consultation with Mursion's executive management team, Legal Counsel, and Information Technology department. Mursion senior management supports all information security policies and mandates contained within and continues to be involved in maintenance of the company's information security program. This commitment is demonstrated through continual participation in Mursion's information security program, assistance with ongoing reviews of security policies, and ongoing enforcement of the requirements and standards contained within this policy.

1.3. Information Security Policy Management

The Information Security Officer is responsible for ongoing review and updates to this information security policy; policy updates must reflect new and emerging threats, changes to Mursion business strategy, or other organizational changes within the company. Any change to this document requires the approval and authorization of Mursion executive management. The information security policy is to be reviewed no less than once per calendar year.

Publication and Dissemination

This document is to be published in a location accessible to all Mursion personnel and is to be distributed within the organization whenever it is modified or updated. The Information Security Officer is responsible for ensuring that all personnel read, understand, and accept this policy at least annually. In addition, this document is to be distributed to all appropriate Mursion partners, vendors, service providers, or other third parties to ensure they comply with the policies and procedures relevant to their business relationship with Mursion.



This document may be distributed outside Mursion (for example, to customers), but only with the express written consent of the Information Security Officer or a member of Mursion executive management.

2. Risk Management

Mursion's Information Security Department maintains processes for ongoing risk management that are intended to proactively identify vulnerabilities within Mursion systems as well as assess new and emerging threats to company operations.

Mursion performs information and technology risk management in accordance with the *Mursion Risk Management Policy*.

2.1. Security Testing

Mursion employs two complementary methodologies for identifying vulnerabilities in its systems and critical business services. The company subjects its systems and applications to periodic security testing and scans in order to proactively detect and address security vulnerabilities and weaknesses. These tests include internal and external vulnerability scans using various tools.

2.2. Monitoring Of Emerging Threats And Vulnerabilities

While testing provides periodic data about the state of information security within Mursion's production environment, it does not provide information rapidly enough to address new and emerging threats, nor does testing address all potential issues. To address this potential weakness, Mursion's Information Security Department also monitors vendor bulletins and security mailing lists in order to receive proactive information about emerging threats.

2.3. Vulnerability Management Program

Regardless of the origin of an identified vulnerability (penetration tests, vulnerability scans, or security bulletins), all security remediation efforts within Mursion are managed using a consistent process. Once the Information Security Department evaluates the severity of the vulnerability and determines that action is required, they will create a request ticket. These individual requests are assigned to the system, application, or platform owners for further investigation and/or remediation.

2.4. Asset Management

Data Management Policies

Data will be managed and handled in accordance with the *Mursion Data Management Policy*.

Acceptable Use of Computing Assets

All use of computing assets is governed by following *Acceptable Use Policy*.

Proper Use Of Electronic Resources

Electronic resources are provided exclusively to assist in conducting business for Mursion. Use of equipment or systems by unauthorized persons is strictly prohibited, and all access to Mursion's systems and data must be approved and provisioned in accordance with Mursion Information Security Policy and other documented access control standards.



Software Restrictions

- Only company-provided or approved software is permitted on Mursion-owned or maintained equipment. No other software is to be installed without prior written permission from IT. Users are expected to use the standard software provided by Mursion, or identify applications they need in the course of their work. Downloading of any executable files or programs which change the configuration of the system must be formally approved by the IT Department.
- Due to copyright infringement and licensing considerations, Mursion also prohibits copying computer software without prior written approval from IT Management. Under no circumstances are users permitted to copy software in violation of license agreements or terms of use. Similarly, employees may not transfer computer software programs from one computer to another without the express written approval from IT Management. Under no circumstances is the software to be duplicated in any way or form, including, but not limited to, the duplication of information for which the Company is the licensee, or installing the software on more than one computer for the user's use outside of a Mursion facility. Any fines incurred due to pirated software usage will be the responsibility of the user.

Proper Use Of Mobile Devices

- These following policies apply to Mursion data as it relates to mobile devices that are capable of storing/transmitting such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. This policy covers any mobile device coming into contact with company data.
- Personal Mobile Devices that are used to access Mursion' network adhere to the following standards:
 - o Mobile devices may be used to access network resources remotely, or store information when necessary for business use.
 - o Mobile Devices must not be left unattended and, where possible, it must be physically locked away or secured.
 - o Wireless, infrared, Bluetooth or other connection features of Mobile Devices should be turned off when not in use.
 - o The storage of user IDs and passwords which allow access to the Mursion' network or systems is prohibited on Mobile Devices unless it is stored using approved encryption methods and is password protected.
 - o Any software applications purchased by Mursion and installed on Personal Mobile Devices must be removed immediately by the user upon termination of employment. Mursion' Sensitive information must be removed from all Mobile Devices immediately upon termination of the assigned user's employment with Mursion.
 - o Any Mursion Sensitive information transmitted to or from the Mobile Device (e.g., wireless or the Internet) must be encrypted.

Network Acceptable Use

- Only Mursion approved computing equipment is permitted on any Mursion network. Users are prohibited from attaching any non-approved device capable of storing or transmitting data to the network without documented approval IT Management. This provision applies (and is not limited to) to mobile phones, tablets, laptops and portable data storage devices.
- No Mursion network or system may be knowingly used for activities that are considered illegal under local, state, federal, or international law.



3. Operations Security

3.1. Operational Procedures And Responsibilities

Mursion individual departments may maintain a separate document containing any specific operational policies and procedures.

3.2. Protection Against Malicious Software

Mursion maintains systems intended to prevent the introduction of malicious software into the company's infrastructure, as well as mechanisms for detecting unauthorized transmission of sensitive company data. The use of anti-virus software is mandatory on all workstations, laptops, servers, except for those running operating systems not normally prone to malicious software (e.g. - Linux or Unix variants). All antivirus clients must be capable of detecting all common forms of malicious software, and must be properly configured to check for detection engine updates at least daily and for virus definition updates hourly. It is a violation of company policy to disable or alter the configuration of anti-virus software on employee workstation.

3.3. Incident Response

Mursion's *Incident Response Plan* details the process for incident handling and response.

4. Access Control

4.1. Business Requirement For Access Control

Establishing and maintaining consistent and effective access controls is fundamental to Mursion's information security strategy. The Information Security Officer will implement commercially reasonable practices and procedures designed, as appropriate, to limit and control access to Protected Information and to information systems used to process or access such information.

Access Control Policy

Access to Mursion Systems and Networks is provisioned and deprovisioned in accordance with the *Mursion Access Control Policy*.

User Responsibilities

Passwords are a critical component of controlling access to Mursion computing assets, and all personnel have an obligation to establish and protect effective and secure passwords. Users must realize that their account and password are used to track actions taken using those credentials, so protecting their account(s) is in each user's best interests.

Individual personnel responsibilities regarding passwords include:

- Choose good passwords. One of the most valuable steps that users can take to help secure Mursion is to use effective passwords. Ideally, passwords will be difficult for others to guess, but easy for each individual to remember. Single words from dictionaries, names of family members, or other common words and names are poor choices for passwords. Some helpful tips on selecting a strong password:
 - o Longer passwords are generally stronger than short ones.
 - o Use phrases that you will remember rather than words with extra characters.
 - o Deliberately misspelling words makes a password harder to compromise.



- Secure your password(s). Each user is responsible for protecting their passwords. Do NOT write passwords down, and take steps to make sure that others cannot read a password as it is entered. In public location, treat passwords similar to ATM PIN codes – take a moment to evaluate your surroundings, and do not enter a password in areas that seem unsafe. Exercise caution when entering passwords into links from e-mail, and ensure that webpages prompting for Mursion passwords are appropriate.
- Do NOT share passwords. Do not share passwords with anyone. This includes co-workers, family members, or the Information Technology Department. There is no reason why anyone needs access to an account other than their own. Never send passwords over e-mail or text messaging.
- Act on suspected compromises. If you think your password has been compromised, whether through suspicious activity on your account, or you suspect someone has your password, take action. Immediately change your password, and notify the Information Technology Department of the suspicious activity.

4.2. Network Services Usage

Personnel are only permitted to access network services and networks to which they have been explicitly granted access. This includes the use of internal and external network services, wireless networks, remote access or Virtual Private Networks (VPNs), restricted networks, third party networks (a.k.a. extranets), and the Internet. Use of these networks and network resources is a privilege; by using network technologies, personnel implicitly agree to the terms of Mursion's security and acceptable use policies. Attempts to intentionally bypass network security controls or infrastructure are prohibited and will result in appropriate disciplinary action. Personnel are not permitted to use network protocols or services that they know may expose Mursion or its systems to undue risk.

4.3. External Network Connections, Vpn, And Remote Access

Networks outside the direct control of Mursion personnel are a potential threat to Mursion's network, and have the potential to compromise some of Mursion's perimeter controls. All connections to external networks are subject to review by the Information Security Department prior to their establishment, and must have documented access controls in place to restrict the flow of data to the external network.

Virtual Private Networks (VPNs) and remote access technology must conform to Mursion standards for acceptable levels of encryption, and may only be used with approval from Mursion management. Personnel should not use VPN software to connect to Mursion's network in locations they suspect may be risky or may expose the company's network to undue risk.

4.4. Secure Log-On Procedures

Secure log-on procedures for production systems will be configured in accordance with the *Mursion Access Control Policy*,

5. Privacy Policy

Mursion's Privacy Policy details the requirements for privacy requirements applicable to Mursion services.



6. Amendment/Termination Of This Policy

Mursion reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the company and its employees, partners, agents and contractors.

7. Exceptions

Requests for an exception to this Policy must be submitted to authorized personnel for approval. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

8. Violations/Enforcement

Any known violations of this policy should be reported to the company's IT department. Violations of this policy can result in immediate withdrawal or suspension of system and Network privileges and/or disciplinary action in accordance with company procedures. The Mursion may advise law enforcement agencies when a criminal offense may have been committed.