MAROPOST®

155 University Ave
Suite 1900, Toronto, ON
M5H 3B7, Canada

T 888.438.3152
F 647.438.5600
maropost.com

# SECURITY POLICY

V 2.0

Date: May 09, 2018

**Table of Contents**

**Revision History**

| Version | Date | Author | Notes |
|---|---|---|---|
| 2.0 | May-09-2018 | Dan Hestad, Manny Ju | Additional items for GDPR coimpliance |
| 1.0 | Feb-08-2017 | Dan Hestad, Manny Ju, Jagdeep Singh | Initial Release |

# 1 Purpose and Scope

Maropost is committed to high standards of excellence for protection of information assets and information technology resources. Without the implementation of appropriate controls and security measures, these assets would be subject to potential damage or compromise to confidentiality or privacy, and the activities of Maropost and its clients are subject to interruption. (Ref: ISO/IEC 27002:2005 Sect. 6.1.1)

The purpose of the Maropost Information Security Program ("Program") is to establish guidelines for achieving appropriate protection of Maropost electronic information resources and to identify roles and responsibilities at all levels. (Ref: ISO/IEC 27002:2005 Sect. 6.1.1)

The provisions in the Program apply to all information subjects and objects subject to GDPR (optionally PCI). This policy (and derivative policies) are based on ISO 27002 standards but designed to conform to and achieve compliance with GDPR. Some entities may be subject to additional federal, state, international law or other regulations.

# 2 Information Security Program Overview

## 2.1 Roles and Responsibilities

To ensure, to the extent possible, the confidentiality, integrity, and availability of Maropost information assets, Maropost has created the Privacy Working Group (PWG). The PWG will consist of a minimum 3 members. The members will represent senior personnel from IT Operations, Business Operations and Human Resources. It may also include a 3rd party representative from an outside consulting firm to lend technical and compliance expertise. The PWG will meet quarterly to review current and future privacy and security related issues. The PWG will also lead the annual risk assessment process. The PWG will be responsible for the implementation of the Security & Compliance Program and periodic evaluation of the Program to ensure that the Program adequately addresses operational or environmental changes (Ref: ISO/IEC 27002:2005 Sect. 6.1.3).

Responsibility for compliance with the Program will rest with a number of individuals, and the PWG must facilitate this compliance through collaborative relationships within Maropost and with its clients and trusted third parties (Ref: ISO/IEC 27002:2005 Sect. 6.1.3).

All Team Members of the Maropost organization are expected to comply with the policies and procedures and to exercise responsibility appropriate to their position and delegated authorities (Ref: ISO/IEC 27002:2005 Sect. 6.1.3) and (PCI DSS v1.2 Sect. 12.4).

All procedures within this Program will be practiced in accordance with Maropost Human Resources policies and guidelines.

## 2.2 Program Objectives

The overall security objectives of the Program are to ensure confidentiality, integrity, and availability regarding IT security. These objectives are the paramount goals for ensuring the protection of information and Resources from unauthorized access, use, disclosure, disruption, modification, or destruction (Ref: ISO/IEC 27002:2005 Sect. 12.3.1).

**Confidentiality**: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The assigned level of confidentiality is used in determining the types of security measures required for its protection from unauthorized access or disclosure.

**Integrity**: guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. The level of impact of unauthorized modification or destruction of information resources determines the importance of maintaining the integrity of a Resource.

**Availability**: ensuring timely and reliable access to and use of information. Emergency management planning must take into account the availability requirements of a particular Resource to determine its inclusion in emergency and disaster recovery planning.

The Program components include:

- Risk assessment strategies to identify vulnerabilities and threats to information resources
- A security plan that includes recommendations for administrative, technical, and physical security measures to address identified risks relative to their sensitivity or criticality,
- Incident response planning and notification procedures, (PCI DSS v1.2 Sect. 12.5.3)
- Guidelines for security awareness training and education as appropriate (PCI DSS v1.2 Sect. 12.6)
- Appropriate review of third-party agreements for compliance with federal, state and international laws and compliance requirements (Ref: ISO/IEC 27002:2005 Sect. 6.1.2).

## 2.3 Risk Assessment

On at least an annual basis, Maropost will conduct a risk assessment to: (PCI DSS v1.2 Sect. 12.1.2):

- Provide an inventory of and the nature of electronic information resources,
- Understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources, and
- Identify the level of security necessary for the protection of the resources (Ref: ISO/IEC 27002:2005 Sect. 4.1).

This risk assessment will:

- Take into account and prioritize the potential adverse impact on Maropost's reputation, operations, and assets,
- Ensure full review and classification of Maropost information assets by the level of security objectives assigned to them,
- Be conducted by qualified personnel,
- Address the appropriateness and frequency of staff and management security awareness training (Ref: ISO/IEC 27002:2005 Sect. 4.1).

After completing the annual risk assessment, an information security action plan will be developed to take into consideration the acceptable level of risk for systems and processes. Appropriate mechanisms to safeguard information will be selected relative to the security objectives determined by the risk assessment. Controls selected to mitigate risks will include administrative, operational, technical, physical and environmental measures as appropriate. The information security plan will identify cost-

effective strategies to be implemented consistent with organizational goals and functions for mitigating that risk. The security plan will account for the management, use, and protection of information that has some level of confidentiality and identify the procedures and controls that will be implemented to enhance security for information assets (Ref: ISO/IEC 27002:2005 Sect. 4.2 and Sect. 12.3.1).

# 3 Administrative Controls

Administrative controls consist of a range of administrative processes and procedures to implement the Program. Workforce controls include appropriate assignment of responsibility within the organization for determination of workforce need to access Resources in order to perform assigned tasks. Responsibility for information security will be identified early in the employment process. Positions that require information technology skills will include an emphasis on security knowledge and skills throughout the hiring and employment process (Ref: ISO/IEC 27002:2005 Sect. 8.1).

In order to ensure compliance with the above requirements, all employees or third party contractors/vendors working with Restricted Data are expected to employ security practices as appropriate to their responsibilities and roles, which include, but are not limited to (Ref: ISO/IEC 27002:2005 Sect. 8.1.1):

- Taking appropriate actions to ensure the preservation of data confidentiality and integrity,
- Taking appropriate precautions to ensure protection of data from unauthorized access, modification, or destruction,
- Complying with license agreements, terms and conditions, and laws pertaining to intellectual property, and
- Complying with identified security procedures.

## 3.1 Authorized Access

Access to all Restricted Data will be granted in a controlled manner based on need to know and subject to the approval of the designated information Data Owner. Team Members will be explicitly granted access to Restricted Data; there is no implicit right of access. Controls have been developed, implemented, monitored and maintained to create accountability and to prevent any compromise of the confidentiality, availability, and integrity of information assets.

In order to ensure authorized access to all employees or third party contractors/vendors working with Restricted Data, the following procedures to have been put in place:

- As part of the hiring process and before receiving access to Restricted Data, Team Members must undergo background checks performed to include criminal checks and verification of employment records. (Ref: ISO/IEC 27002:2005 Sect. 8.1.2).
- Authorized access, both logical and physical, shall only be granted to those Team Members who have a legitimate business reason to access specific Resources (Authorized Individuals) (Ref: ISO/IEC 27002:2005 Sect. 8.1.1).
- Upon hire, a new Team Member's Supervisor will review and propose access. Data Owner must approve in writing any request for authorization and assignment of the associated level of privilege. Records of this approval will be retained. Data Owners must not approve their own access.

- Team Members must sign the Maropost Written Information Security Program (Defined in Definitions section) acknowledgement prior to being granted access to Maropost Restricted Data and reconfirm on an annual basis.
- Access for Team Members who change roles or transfer to other areas of Maropost should be immediately given the access required for the new role. Access that is no longer required for the new role should be removed or disabled immediately. (Ref: ISO/IEC 27002:2005 Sect. 8.1.3).
- When access is granted, Team Members are responsible for all system activity under their unique account and have the responsibility to protect their account by creating and maintaining passwords compliant with the Maropost Acceptable Use Policy. In addition, Team Members are responsible for maintaining the confidentiality of their unique ID and password by not sharing it with any other party.
- Maropost will re-evaluate the privileges granted to users annually to ascertain that the access is still commensurate with the user's job responsibilities. User accounts found to be invalid should be disabled.
- Non-employee user accounts and access privileges, including third parties, contractors, consultants, and temporaries, shall be re-evaluated every six months. User accounts found to be invalid should be disabled.
- In the event of disciplinary action where there is a concern that access to Resources endangers the integrity of such Resources, management will review and act to restrict, suspend or terminate access (Ref: ISO/IEC 27002:2005 Sect. 8.2.3).
- Upon termination or when job duties no longer require a legitimate business reason for access, all access will be revoked. Further for Team Members who announce their decision to terminate, access may be removed if continued access may result in an unacceptable level of risk. Access shall be revoked for individuals on a leave of absence. (Ref: ISO/IEC 27002:2005 Sect. 8.3.3)
- Upon termination, Supervisor will ensure disposition of electronic information resources (Ref: ISO/IEC 27002:2005 Sect. 8.3.2).
- During any extended leave of absence, access privileges should be revoked or restricted, as appropriate.

## 3.2 Acceptable Use

Maropost has developed usage policies for critical Team Member-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. (Ref: ISO/IEC 27002:2005 Sect. 7.1.3)

In order to ensure acceptable usage of critical technologies, all employees, contractors, consultants, temporary and other workers at Maropost, including all personnel affiliated with third parties must adhere to the Maropost Acceptable Use Policy. This policy applies to information assets owned or leased by Maropost, or to devices that connect to a Maropost network or reside at a Maropost site such as personal mobile devices used to access Maropost information or network. (Ref: ISO/IEC 27002:2005 Sect. 7.1.3, ISO/IEC 27002:2005 Sect. 11.7.2 and PCI DSS v1.2 Sect. 12.3)

### 3.3 Violations

It is a violation of Maropost policy for individuals to attempt to gain unauthorized access to Resources or in any way willfully damage, alter, or disrupt the operations of Resources (Ref: ISO/IEC 27002:2005 Sect. 5.1.1). It is also a violation of Maropost policy for individuals to capture or otherwise obtain or tamper with passwords, encryption keys, or any other access control mechanism that could permit unauthorized access, except where expressly required in the performance of their duties (Ref: ISO/IEC 27002:2005 Sect. 5.1.1).

In order to ensure compliance with the above requirements, the following procedures have been put in place:

- Supervisors and department heads are responsible for promptly reporting any known or suspected policy violations of the provisions in this policy to the Data Owner or Custodian (Ref: ISO/IEC 27002:2005 Sect. 13.1.1).
- Team Members who become aware of the occurrence of any violation should report the violation promptly to their supervisor, department head. Data Owners or Custodians should be notified of such violations in accordance with departmental procedures (Ref: ISO/IEC 27002:2005 Sect. 13.1.1)
- Data Owners may withdraw the privileges of any individuals who violate these policies if, in their opinion, continuation of such privileges threatens the security (confidentiality, integrity, and availability) of restricted or Essential Resources (Ref: ISO/IEC 27002:2005 Sect. 8.2.3)
- Depending on the nature of the violation and the likelihood of a recurrence, the Data Owner or Custodian shall take prompt action to protect against future violations to the extent feasible, and/or remove the means by which the violation occurred (Ref: ISO/IEC 27002:2005 Sect. 8.2.3).
- In the event of a violation of the provisions in this policy that involves possible unlawful action by an individual, the employee's immediate supervisor, or other appropriate official should immediately be notified. Notification should take place before any action is taken, unless prompt emergency action is required to prevent bodily harm, significant property loss or damage, loss of significant evidence (Ref: ISO/IEC 27002:2005 Sect. 13.1.1).
- Maropost reserves the right to revoke access to any Resource for any individual who violates the provisions of this policy (Ref: ISO/IEC 27002:2005 Sect. 8.3.1).

## 4 Identity and Access Management

This section addresses security measures related to controlling access to Resources through operational or technical measures, e.g., passwords, configuration settings, software or network controls, controls related to software development and change management, security of data and communications, and controls to reduce risk from known threats and malicious programs (Ref: ISO/IEC 27002:2005 Sect. 11.1).

Selected technology will be adequate to ensure sufficient protection commensurate with the level of risk ascribed to the electronic information resource and the magnitude of harm that would result from the loss, misuse or unauthorized access to or modification of information. The selected technology will be supported by operational controls designed to ensure that the Resource is adequately protected (Ref: ISO/IEC 27002:2005 Sect. 8.1.1).

Maropost access control measures include secure and accountable means of authorization and authentication.

Authorization is the process of determining whether or not an identified individual or class has been granted access rights to an information resource and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.

Authentication is the process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.

## 4.1 Access Controls

Access controls are put in place to restrict Resource access to Authorized Individuals. Such mechanisms will be implemented to ensure that security objectives are in compliance with federal, state and international law. This includes not only the primary operational copy of the information, but also data extracts and backup copies. Authorized Individuals and their specific level of privilege should be specified by the Data Owner, unless otherwise defined by Maropost policy.

Records of access events are to be maintained consistent with audit log guidelines (Ref: ISO/IEC 27002:2005 Sect. 10.10.1)

Rights of access to modify data are to be performed according to procedures that ensure data integrity. Exceptions may be made on a case-by-case basis but should always be performed in a controlled manner and with the knowledge of the Data Owner (Ref: ISO/IEC 27002:2005 Sect. 10.1.3).

## 4.2 Password Authentications

Appropriate password management conventions, including periodic identification of weak passwords, password encryption, and other security measures as deemed appropriate shall be identified. Passwords and other authentication credentials are considered Restricted Data and require the highest level of security protection whether in storage or transit (Ref: ISO/IEC 27002:2005 Sect. 11.2.3).

In order to ensure compliance with the above requirements, the following procedures have been put in place:

- Supervisors and department heads are responsible for promptly reporting any known or suspected policy violations of the provisions in this policy to the Data Owner or Custodian (Ref: ISO/IEC 27002:2005 Sect. 13.1.1).
- Passwords selected by individuals or automatically generated to protect access to information resources should be difficult to ascertain and should comply with Maropost password standards. (Identification & Authentication Standard).
- Passwords to individual accounts should never be shared with other individuals unless specifically approved and documented as an exception to policy by Data Owners responsible for the Resources to be accessed.
- Maropost Password Standards: Passwords must be a minimum of 8 characters and contain at least one alphabetic, one numeric, and one special character. No two characters may sequentially repeat, either.
- Passwords must be changed regularly. The change interval should not exceed 90 days.

- Passwords must not be inserted into email messages or other forms of electronic communication unless protected.

### 4.3 Session protection

Technical security mechanisms should be in place that prohibit or minimize the risk of unauthorized access to Resources by others who might gain control of the working session, for example, by accessing the Authorized Individual's computer if that individual leaves it unattended. Measures such as secure screensavers, automatic logout, and/or other means of session protection should be operative on all devices with access to restricted Resources. (Ref: ISO/IEC 27002:2005 Sect. 11.5.5) and (PCI DSS v1.2 Sect. 12.3.8).

In order to ensure compliance with the above requirements, the following procedures have been put in place:

- Sessions should be set to timeout automatically after 15 minutes of inactivity

## 5 Systems and Application Security

### 5.1 Systems Personnel

Responsibility for systems and application security will be assigned to an individual knowledgeable about the information technology used in the system and in providing security for such technology. This individual will determine security plans as appropriate to the supported systems, applications, and data (Ref: ISO/IEC 27002:2005 Sect. 11.6) and (PCI DSS v1.2 Sect. 12.5.1).

Maropost designated Team Members who manage, operate, and support system and application security ("Systems Personnel"), are expected to follow all applicable Maropost policies, and use appropriate professional practices in providing for the security of the systems they manage.

In addition to periodic risk assessments, Systems Personnel will routinely evaluate Resource exposure to potential and known threats and deploy controls commensurate with the level of risk and magnitude of the harm that could result from loss, misuse, or unauthorized access to supported systems, applications, and data (Ref: ISO/IEC 27002:2005 Sect. 12.6.1).

The principle of separation of duties will be employed to ensure that responsibilities for critical functions are divided among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such controls keep a single individual from subverting a critical process.

### 5.2 Backup and retention

Sound professional system administration practices require the implementation of routine backup of applications and data ((Ref: ISO/IEC 27002:2005 Sect. 10.5).

The following procedures shall be in place to ensure the routine backup of the Maropost applications and data:

- Backups will be automated.
- For Web app, backup is scheduled weekly.
- All data is automatically encrypted prior to persisting to storage and decrypts prior to retrieval.

- Backup will be retained for 30 days unless otherwise required.

All backup and other retention services for data will comply with Maropost policies regarding data retention (Ref: ISO/IEC 27002:2005 Sect. 15.1.3).

### 5.3 System protection

Measures should be deployed to limit access to systems that host restricted or Essential Resources and to protect systems from “malicious software” (Ref: ISO/IEC 27002:2005 Sect. 11.6).

Maropost deploys the following procedures to ensure that host restricted or Essential Resources and systems are protected from “malicious software” (Ref: ISO/IEC 27002:2005 Sect. 11.6).

- Antivirus and malicious code detection tools will be installed and active.
- Activities are monitored and controlled on a regular basis.

## 6 Change Management

Maintaining system integrity requires that all changes to a system are conducted according to a planned and supervised change management process. In particular, changes to any Restricted or Essential Resource shall be performed according to authorized change management procedures that ensure the recording of all changes. (Ref: ISO/IEC 27002:2005 Sect. 10.1.2)

In order to ensure compliance with the above change management requirements, the

Maropost Change Management procedures include:

- monitoring and logging of all changes,
- steps to detect unauthorized changes,
- confirmation of testing,
- authorization for moving application programs to production,
- tracking movement of hardware and other infrastructure components,
- periodic review of logs,
- back out plans, and
- user training.

## 7 Encryption

Suitably strong encryption measures shall be employed and implemented, whenever deemed appropriate, for information in storage and during transmission (Ref: ISO/IEC 27002:2005 Sect. 12.3.1).

In order to ensure compliance with the above requirements, the following encryption procedures have been put in place:

**Transit** -- Restricted Information shall be encrypted during transmission using measures strong enough to minimize the risk of the information’s exposure if intercepted or misrouted for example HTTPS and Transport Layer Security.

**Storage** -- Application data shall be stored with encryption at rest. Encryption shall be performed at the database level and storage level.

Restricted Information may not be retained on portable equipment. (Ref: ISO/IEC 27002:2005 Sect. 12.3.1).

### 7.1 Key management

Maropost shall implement encryption key management plans to ensure the availability of encrypted authoritative information (Ref: ISO/IEC 27002:2005 Sect. 12.3.2).

The encryption key management plan shall ensure that data can be decrypted when access to data is necessary. This requires key backup or other strategies to enable decryption, thereby ensuring that data can be recovered in the event of loss or unavailability of cryptographic keys.

The encryption key management plan shall address handling compromise or suspected compromise of encryption keys. In addition, the plan should address the impact of a key compromise on system software, hardware, other cryptographic keys, or encrypted information.

The encryption key management plan shall include a process to determine whether any encryption keys may have been compromised as a result of any security incident.

The encryption key management plan shall include periodic review to ensure suitably strong encryption.

Users shall be made aware of their unique role if they are given responsibility for maintaining control of cryptographic keys.

Background checks shall be conducted for Maropost employees who control and manage encryption keys and key management software and hardware (Ref: ISO/IEC 27002:2005 Sect. 8.1.2).

## 8 Physical and Environmental Controls

Establish procedures for the physical protection of its Resources. All facilities hosting restricted or Essential Resources should conform to the following recommended guidelines commensurate with the level of risk. Appropriate locking or other physical security mechanisms should be implemented for all equipment vulnerable to unauthorized removal (Ref: ISO/IEC 27002:2005 Sect. 9.1) and (PCI DSS v1.2 Sect. 9.1).

All physical hosting facilities should implement appropriate measures for the prevention, detection, early warning of, and recovery from emergency conditions, including, but not limited to, earthquake, fire, water leakage or flooding, disruption or disturbance of power, air conditioning failures, and environmental conditions exceeding equipment limits. Procedures should include measures to protect Resources from theft, damage, or improper use (Ref: ISO/IEC 27002:2005 Sect. 9.1.4).

### 8.1 Physical Access Controls

Controls for limiting physical access to facilities housing Restricted or Essential Resources should be implemented through the use of combination locks, key locks, badge readers, manual sign in/out logs, verification of identification, etc. The ability to track both ingress and egress of all individuals should be maintained as appropriate (Ref: ISO/IEC 27002:2005 Sect. 9.1.2).

Limiting physical access to facilities may also include technical mechanisms, such as use of proximity card readers. In those instances, technical access control guidelines apply (PCI DSS v1.2 Sect. 9.1.1).

Records of access events should be maintained consistent with audit log requirements (PCI DSS v1.2 Sect. 9.1.1).

Entry to a data center must be able to be tracked to an individual with at least the following information:

- Name
- Time entered
- Time exited

Monitoring cameras shall be in place inside the physical data center (PCI DSS v1.2 Sect. 9.1.1)

## 8.2 Tracking Reassignment or Movement of Devices and Stock Inventories

Procedures should be implemented that (Ref: ISO/IEC 27002:2005 Sect. 9.2.6):

- track the receipt, reuse, and removal of hardware and electronic media, including documentation of hardware reassignment. Removal of restricted or other sensitive information should be conducted in accordance with procedures below regarding final disposition of equipment.
- maintain records documenting repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, and locks.

## 8.3 Disposition of Equipment

Procedures should ensure implementation of controls to address the re-assignment or final disposition of hardware and electronic media, including requirements that ensure complete removal of restricted or other sensitive information as appropriate, such as by shredding, overwriting a disk, or employing professional data destruction services as commensurate with risk. Sufficiently strong disk encryption may be used as an alternative mitigation. If electronic media or hardware is subject to a litigation hold, final disposition of these resources must be conducted in such a manner that ensures that relevant data is not lost (Ref: ISO/IEC 27002:2005 Sect. 9.2.7).

## 8.4 Portable Devices and Media

Maropost will establish procedures to ensure physical security for portable devices and media housed within their immediate work area or under their control, such as laptop computers, PDAs, memory sticks, CD ROMs, etc. (Ref: ISO/IEC 27002:2005 Sect. 11.7.1)

In order to ensure compliance with the above requirements, the following encryption procedures have been put in place:

- With the exception of Maropost Third Party Sensitive data, Restricted Information may be retained on portable equipment only if protective measures, such as encryption, are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment.
- No Maropost Third Party Sensitive data should be retained on portable equipment.

# 9 Incident Response Planning and Notification Procedures

Maropost has established and implemented procedures to ensure the ability to respond expeditiously to known information security breaches, disruptions caused by failure of a security mechanism and known or suspected security incidents. (Ref: ISO/IEC 27002:2005 Sect. 13.1.1), (PCI DSS v1.2 Sect. 12.9.1) and (PCI DSS v1.2 Sect. 12.5.3)

Maropost's goal for incident response is to minimize any negative impact to our clients through the use of a comprehensive response and mitigation plan. This plan includes mechanisms for documenting the incidents, determining notification requirements, implementing remediation strategies, and reporting to management. (PCI DSS v1.2 Sect. 12.9)

Sensitive data (PII, Cardholder data, etc) will not be collected unless necessary for business purposes.

An Incident Response Team will be formed. The team will include representatives from:

- IT
- Legal
- HR

Upon indication that an incident may have occurred the IR Team will be activated

The 2 top priorities of the HR Team are:

1. Minimize Damage
2. Report complete factual analysis to stakeholders

# 10 Education and Training

The PWG and supervisors shall ensure that appropriate security awareness training is routinely conducted for all employees who handle sensitive data (Ref: ISO/IEC 27002:2005 Sect. 8.2.2) and (PCI DSS v1.2 Sect. 12.6)

In order to ensure compliance with the above requirements, the following educational procedures have been put in place:

- Training programs will be conducted within 30 days of hire and at least annually for all employees. Program will include a review of Maropost security policy, guidelines, procedures, and standards, as well as departmental procedures and best practices established to safeguard sensitive information.
- Training shall be in conformance with regulations governing specific categories of Restricted Information
- Training materials should include topics such as password management and use, best practices for protecting restricted information, incident reporting, and security reminders regarding current threats to technical environments in which individuals are working.

# 11 Third-party Agreements

When agreements are established with contractors, consultants, or external vendors, those agreements shall include satisfactory assurances that the contracting third party will appropriately safeguard

Maropost information in accordance with federal and state laws and regulations and Maropost policies. (Ref: ISO/IEC 27002:2005 Sect. 6.2.3 and 6.2.1)

When providing access to or passing Restricted Information to a third party agent of Maropost, the written contractual agreements should include terms and conditions that:

- Prevent disclosure of Restricted Information by the agent or affiliate to other third parties including subcontractors, except as required or permitted by the approved Maropost agreement or contract terms,
- Require all agents and affiliates to observe federal and state laws and Maropost policies for privacy and security,
- Require a specific plan by the agent or affiliate for the implementation of administrative, technical, or physical security strategies as outlined in this policy,
- Require a plan for the destruction or return of Restricted Information upon completion of the agent's or affiliate's contractual obligations,
- Specify access or authorization permissions and restrictions necessary to fulfill contractual obligations,
- Require notification of any breach of the security of personal information to the Maropost owner of computerized data immediately following discovery if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

Access to Maropost or derivative information should be terminated when contractual obligations have been completed.

# 12 Appendix A - References

Management Guide for Information Security

ISO 27002

PCI DSS v3.2

General Data Privacy Regulation (EU) 2016/679

OWASP Guidelines

SANS Security Configuration Guidelines

# 13 Appendix B – Definitions

**Authorized Individual**

An Maropost employee, contractor, or other individual affiliated with Maropost who has been granted authorization by a Data Owner, or his or her designee, to access a Resource and who invokes or accesses a Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with Maropost. The authorization granted is for a specific level of access to a Resource as designated by the Data Owner, unless otherwise defined by Maropost policy.

**Information Security Program (Document listing)**

The following documents make up the Information Security Program. Users should sign/acknowledge on an annual basis receipt of these documents if required.

- Information Security Policy
- Acceptable Use Policy
- Completion of Annual security training
- Other documents as appropriate (for example – developers should review the secure coding policy)

**Data Custodian**

The authorized Maropost personnel who have physical or logical control over a specific Electronic Information Resource. This role provides a service to a Data Owner.

**Data Owner**

The individual designated responsibility for the information and the processes supporting a specific Maropost function. Data Owners are responsible for ensuring compliance with federal or state statutory regulations. Responsibilities of Data Owners may include, for example: specifying; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which individuals may have access to an application or to data accessible via an application.

**Electronic Information Resource (Resource)**

A resource used in support of Maropost activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data (in raw, summary, and interpreted form), other electronic files, and associated computer server, desktop (workstation), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives), communications and other hardware used to conduct activities in support of the Maropost mission. These resources are valued information assets of Maropost.

**Encryption**

The process of converting data into a cipher or code in order to prevent unauthorized access. The technique obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher. The keys are binary values that may be interpretable as the codes for text strings, or they

may be arbitrary numbers. Appropriate management of these keys allows one to store or transmit encrypted data “in plain sight” with little possibility that it can be read by an unauthorized entity. For example, encryption can protect the privacy of restricted data that is stored on a laptop computer, even if that laptop computer is stolen. Similarly, it can protect data that is transmitted, for example, over a network, even if that network is tapped by an unauthorized third party

**Essential Resource**

A Resource is designated as Essential if its failure to function correctly and on schedule could result in (1) a major failure by Maropost to perform a mission-critical function, (2) a significant loss of funds or information, or (3) a significant liability or other legal exposure to Maropost or an Maropost client.

**Restricted Information**

Restricted Information describes any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

**Restricted Resource**

A Resource that supports the storage, transmission, or processing of restricted information to which access requires the highest degree of restriction and that requires the highest level of security protection.

**Team Member**

Employees or third party contractors/vendors of Maropost