Paperless Transaction Corporation

Corporate Security Policy

Table of Contents

Review Dates:

12/14/2012 – Bobby Hestand – IT Manager

11/17/2013 – Bobby Hestand – IT Manager

1 Introduction

Paperless Transaction Corp (“PTC”,“Company”) computer information-system resources (“Company IT Resources”) are a valuable Company asset and must be managed accordingly to ensure their integrity, security, and availability for lawful business activities.

Of critical importance in carrying out this mission is establishing basic information security policies and standards for managing PTC’s information, while providing both access and reasonable security at an acceptable cost. Also of significant importance is the underlying philosophy that these policies and procedures are in place to facilitate and support authorized access to Company information.

The information security community defines information system security in terms of protecting the Confidentiality, Integrity, and Availability (CIA) of information. By using PTC’s Security Policies, the Company strives to achieve these goals for all Company information.

- **Confidentiality** ensures that information is not disclosed to unauthorized persons or processes.
- **Integrity** is the prevention of information modification by unauthorized users and the prevention of the unauthorized or unintentional modification of information by authorized users.
- **Availability** ensures that a system’s authorized users have timely and uninterrupted access to the information in the system.

What follows is the *Corporate Security Policy*. In this document, there are *Functional Policies* that contain procedures, standards, and guidelines for use in implementing and maintaining integrity, availability, and confidentiality for the Company. A policy is a statement of management’s intent; its implementation is mandatory.

2 Scope

The following security policies apply to all computing platforms, including local area networks, wide area networks, server systems, desktop computers, laptops, and applications used to process PTC’s information. Policies also apply to users of those systems and applications, including those who install, develop, maintain, administer, and use those systems and applications for the Company and its corporate adjuncts.

All users of PTC’s-supplied technology facilities and resources will abide by all applicable Company, State, and Federal guidelines, policies, regulations, statutes, and procedures pertaining to security and privacy. Anyone accessing Company data is personally responsible for proper use of the resulting available information. All users must comply with and abide to all policies contained within this document. All users must acknowledge and agree to abide by the *PTC’s IT Resource Acceptable Use Policy* by signing the document.

All data, programs, systems, and procedures (hereafter called "information" or “systems”) gathered, stored, or maintained for PTC’s purposes, are the property of PTC’s, unless otherwise stated in a contractual agreement.

Any person, group, or custodian accessing Company information must recognize the responsibility to preserve the security and integrity of this information. Such information shall be used only for conducting Company business or as appropriately authorized.

3 Policy Development and Maintenance

This section describes the process for developing, maintaining, and implementing policy and procedures for accessing, storing, and using electronic information.

3.1 Policy Administration

Information Technology is responsible for administering this policy. The Director of Information Technology reviews and approves all changes.

3.2 Changes to Policy and Standards

All requests to change policies and standards must be received in writing and contain brief, factual comments describing the problem, recommendations, and benefits of the proposed change.

3.3 Exceptions to Policy and Standards

If an exception is required, the requestor will request an exception from the IT department in writing. This request will contain a description of the variance, the risk associated with the variance, a sunset date, and remediation plan. Each request must be signed off before the variance to the policy is allowed. Any variance that is designed to be over a year on duration may represent a motion to review and possibly modify the existing policies, or develop an alternative technological solution that falls within policy. The Security Manager retains all such requests, for audit purposes.

4 General Procedures

4.1 Security

4.1.1 Physical/Datacenter Access

Corporate production servers must be located in a secure physical location with access only for authorized personnel by using a combination lock, key lock, access card, guard or combination of these. The location must have adequate and redundant power and environmental controls to ensure a stable and effective computing environment.

4.1.2 Firewalls

Firewalls must separate corporate computers and servers from the Internet and vendors with logical and/or physical circuits connecting to PTC's network. See the *Firewall Configuration Standards* document for more information.

4.1.3 Intrusion Prevention/Detection

The intrusion prevention/detection system (IPS/IDS) must monitor traffic to protect Internet-facing systems and alert Information Security of suspected compromises. Information Security personnel must ensure that all definitions for the IPS/IDS engine are current.

4.1.4 User Security

All users must have a separate user account and password that must be kept secret. Users cannot share accounts. NEVER COMMUNICATE INDIVIDUAL ACCOUNT PASSWORDS TO ANYONE. THE INFORMATION TECHNOLOGY DEPARTMENT WILL NEVER ASK FOR USER PASSWORDS**.**

Users must *software lock* their workstations when unattended. To lock a workstation, press the CTRL-ALT-DEL keys and select *Lock Computer* or press the Windows key and L at the same time for Windows XP machines or later.

Remote users must be authorized and agree to the PTC's *Remote Access Policy.*

Users may not access another user's data without permission. Each server must have a file protection system that restricts user access to the user's own files. Exceptions include a user belonging to a group that has file access through group file permissions.

4.1.5 Data Security

All confidential and restricted corporate data must be encrypted before being transmitted over a public communications channel. See Data Handling standards located in this policy at section 6.5.

All restricted corporate email must use encryption. Day-to-day email does not require encryption. See Data Handling standards located in this policy at section 6.5.

4.1.6 Patch Management

All servers and workstations must have the most current security patches applied within 30 days of vendor patch release with the least impact to availability of these systems. Security patches should be tested prior to release to ensure compatibility. All windows patching is handled via Firehost's Security team using the IPMI interface.

4.1.7 Credit Card Data

The *full contents* of any credit card track (from the magnetic stripe on the back of the card) must not be stored in databases, log files, or point-of-sale products. This includes storing the card-validation code (three-digit value printed on the signature panel of a card). Credit numbers displayed on systems or printed out should have all but the last 4 digits masked. Credit card numbers (in databases, logs, files, backup media, etc.) are to be stored securely; for example by means of encryption or truncation. Transmission of full credit card account numbers via clear text methods of data transmission (such as email, ftp) are to be encrypted using industry standard strong encryption algorithms.

4.2 Integrity

Only users accounts contained within the Administrator group may access all files not classified as restricted. Only the Information Security group will have access to Restricted data for purposes of administration and auditing.

Servers that contain data must keep logs of user and system activity.

All systems must have anti-virus software installed that scans all disks, removable drives, incoming traffic, and files.

Restricted data must be encrypted during data transfer. See Data Handling standards located in this policy at section 6.5.

Desktop workstations will have standardized configurations for each department that will include designated versions of the operating system at the specified revision level and specified anti-virus software.

4.3 Availability

Dial-in/VPN capability will be limited to specified servers that will authenticate the user and ensure encrypted communications. Refer to the *Remote Access Policy*.

An employee's supervisor must request the issue of portable computers. Usage is restricted to business purposes. Users must be aware of and accept the terms and conditions of use, including the responsibility for the information held on such devices.

Only Company approved or Company supplied equipment can connect to the system.

Each server must be connected to an uninterruptible power supply (UPS).

All servers must have a targeted service level.

All servers must be in a room with controlled access.

Access to servers on the internal network from remote systems must be restricted by a firewall and is subject to authentication.

A business continuity plan will be maintained that meets stated business requirements and is validated through testing.

4.4 Accountability

All account security events must be logged.

All Restricted file access must be logged.

All Restricted data sent to remote systems must have an associated digital signature. See Data Handling standards located in this policy at section 6.5.

All software deployed on servers or workstations must be authorized by the Information Technology Department. A log of installed software must be maintained.

All connections through the firewall must be logged.

4.5 Recovery

All server data will be backed up daily using incremental or differential backups.

Full backups will be performed once a week.

Archives will be performed monthly and once a year.

The most recent weekly backups and archives must be stored off-site.

4.6 Education

The Information Security group will provide information security training.

Security related events, such as virus outbreaks, will be communicated as necessary to the Information Technology Department and when possible be posted on the PTC Intranet for Company wide education.

Each time an employee or Company-approved third party attempts to log on the Company network, the individual must acknowledge agreement to the following statement banner.

```
Do not attempt to log on unless you are an authorized user.
All information is intended for and may be used only by
PTC employees and authorized representatives.
Copying of software is not permitted.
Hardware or software may not be removed from the Company's
premises without written permission.
Personal software is not permitted.
```

```
No uploading or downloading of any non-company
software or data is permitted.
Only authorized personnel are to perform physical or software
maintenance.
All Data, software, and email on this computer are the property of
Paperless Transaction Corp.
The Company may intercept, monitor, copy, review, delete, or download
any communications or files on this system.

By Logging on to this system you are agreeing to these policies.
```

5 Access Control

A principle concern in the practice of information security is controlling what persons or programs can access which systems. In addition, the privileges that a subject has to a system must be defined. Individuals are given different roles in information classification. The Company uses these roles as summarized in the following sections.

5.1 Data Owner-Directors and Department Heads

An information owner may be an executive or director of a department. This person is responsible for the information that must be protected. The owner has the final corporate responsibility for data protection to protect sensitive information. However, the day-to-day function of data protection is assigned to a Data Custodian.

The Data Owner:

- Makes the original determination about what level of classification the information requires, based on the Company’s data classification scheme.
- Periodically reviews, with the Data Custodian, classification assignments and makes alterations, as business needs change.
- Delegates the data protection duties to the Data Custodian.
- Ensures that unit employees understand security policies, procedures, and responsibilities.
- Approves appropriate data access, allowing staff to complete business-related assignments.
- Reviews, evaluates, and responds to all security violations reported against staff and takes appropriate action.
- Communicates to appropriate Company departments when employee departures, arrivals, and changes affect computer access.
- Assigns a liaison between the Data Custodians and System Administrators.
- Ensures that security procedures are in place to protect information assets under the control of the Data Custodians and System Administrators.

5.2 Data Custodian

The Data Custodian functions as trustee of a portion of the Company's information. For each centrally maintained application, the Director or Department Head of a business unit has the authority to make decisions related to the development, maintenance, operation of, and access to the application and data associated with that business activity. A director or department head may delegate custodial duties to an individual.

The Data Custodian:

- Maintains detailed knowledge of the data within their trust.
- Interprets pertinent laws and Company policies to classify data and define its level of sensitivity.
- Defines required levels of security, including those for data transmission.
- Develops guidelines for requesting access.
- Reviews and authorizes requests.
- Establishes measures to ensure data integrity for access to data.
- Provides data descriptions to inform data users about available shareable data, how to access the data, and what the data means.
- Promotes accurate interpretation of data and publicizes the rules and conditions that could affect the accurate presentation of that data. Reviews usage information.
- Assists with disaster recovery planning and business continuity.
- Defines criteria for archiving data, to satisfy retention requirements.

5.3 Technology System Owner (TSO)

The Technology System Owner (TSO) is a manager from Corporate Information Technology or a Business Unit Technology Support department responsible for the technical maintenance and support of the business application. The TSO is responsible for ensuring the overall appropriateness of Information Technology staff access that may be required to support the application.

- Periodically reviews and validates administrative and non-administrative IT access to the production system and data is appropriate.
- Periodically reviews and validates production batch jobs running on technology resources.

- Responsible for ensuring that approved change management policies are being followed and that the necessary Information Security reviews, approvals and change control sign-offs have been obtained prior to implementing system or application enhancements.

For those systems under its custodianship, the Information Technology Department is responsible for the operating system and application components, including production, system and test libraries, system and test data, and data dictionaries.

Note: The end user/client department has custodial responsibility for production data, including test data.

For systems not supported by the Information Technology Department, custodial assignments are the responsibility of the end user/client department.

5.4 End User

An *End User* (User) routinely uses the protected information as part of their job. Users must follow the operating procedures that are defined in Company policies and they must adhere to the published guidelines for its use.

Note: Users will be granted access on the principle of Least Privilege, which states that a user will be given only enough access necessary for a person to do their job.

6 Information Classification

PTC classifies its data as described in the following sections. If a system contains data or more than one sensitivity class, the system must be classified according to the most sensitive data on the system.

6.1 Public Information/Unclassified

Data on these systems could be made public without any implications for PTC.

6.2 Private Information

External access to private information is to be prevented. Should this data become public, the consequences are not critical. Internal access is selective as chosen by the Data Custodian.

- The unauthorized disclosure of information could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals.
- The unauthorized modification or destruction of information could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals.
- The disruption of access to or the use of information or an information system could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals.

6.3 Confidential Information

Data in this class is confidential within the Company and protected from external access. If such data were to be accessed by unauthorized persons, it could influence the Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Data integrity is vital.

- The unauthorized disclosure of information could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals
- The unauthorized modification or destruction of information could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals.
- The disruption of access to or the use of information or an information system could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals.

6.4 Restricted Information

Unauthorized external or internal access to this data would be grave to the Company or National Security. The number of people with access to this data should be very small. Very strict rules and audit procedures must be adhered to in the usage of this data.

- The unauthorized disclosure of information could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals.
- The unauthorized modification or destruction of information could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals.
- The disruption of access to or the use of information or an information system could be expected to have a *severe or catastrophic* adverse effect on organizational operations.

6.5 Data Handling Standards

	Public	Private	Confidential	Restricted
Criteria	Data on these systems could be made public without any implications for the company (i.e. the data is not confidential), data integrity and confidentiality is not vital.	External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. the company may be publicly embarrassed). Internal and External access is selective, data integrity and confidentiality should be considered significant, but not vital.	Data in this class is confidential within the company and protected from external access. If such data were to be accessed by unauthorized persons, it could influence the company's operational effectiveness or safety, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence. Data integrity and confidentiality is vital.	Unauthorized external or internal access to this data would be critical to the company. Data integrity and confidentiality is crucial. The number of people with access to this data should be very small. Very strict rules must be adhered to in the usage of this data.
Examples	Applications without confidential data, company or product brochures widely distributed data available in the public domain anyway.	Non-sensitive customer or employee information, normal business documents and memos, project/meeting protocols, internal telephone books.	Salaries, personnel data, accounting data, passwords, information on corporate security weaknesses, most customer data, confidential contracts, safety and security documents, government regulated information, credit card information.	Strategic corporate plans, undisclosed financial information, business documents which need a very high level of control and protection.
Minimum Handling Standards	No controls needed. Public data.	Access Control Lists with individual accountability. Data Custodian to approve access.	Access Control List with individual accountability, must use TSL or SSL encryption v3 for web based applications, encryption on databases, encryption for communications outside of network. Data Custodian to approve and review access.	Tightly controlled and monitored Access Control Lists with individual accountability. Not to be published via Extranet/Intranet without expressed permission of department VP. Must use TSL or SSL encryption v3 or greater for web based applications, IT Security to be notified and security to be reviewed. Data sent to another machine outside the Company must have a digital signature associated with it. Data Custodian and Owner to approve and review access.

7 Information Security Responsibility

All electronic information is the property of PTC, unless otherwise stated in a contractual agreement. The following is a summary of responsibilities of those units and/or individuals using or supporting Company information.

7.1 Security and Compliance

Security and Compliance is the unit in the Information Technology Department that is responsible for managing information security standards, procedures, and controls intended to minimize the risk of loss, damage, or misuse of electronic data supported by the PTC Information Technology department.

Among other duties, Business Continuity and Security:

- Provides Company wide leadership, ,coordination, and development of information security policies.
- Helps business units comply with established Company standards and policies, to ensure data integrity.
- Manages security standards, procedures, and controls for Information Technology supported Company information and assets.
- Establishes and maintains high-level standards and related procedures for access to Company information and systems.
- Ensures the security of information managed by the Information Technology Department and implements access as authorized by Data Custodians.
- Assists Data Custodians in identifying and evaluating information security risks.
- Provides training, assistance and support to Data Custodians, Technology System Owners, and System Administrators to ensure security objectives are met for the protection of corporate systems and applications.
- Performs an annual formal risk assessment that identifies threats, vulnerabilities and recommendations.
- Selects, implements, and administers controls and procedures to manage information security risks.
- Manages and monitors security of host systems, platforms, communication mechanisms and other resources that are owned and managed by Information Technology.
- Distributes security report information in a timely manner to Information Technology management, business-unit security contacts, Data Custodians, and appropriate Company administrators.
- Serves as the Information Technology Department focal point for reviewing data security issues that have Company wide impact.
- Responding to incidents and investigating violations of security policies or suspected security breaches of PTC systems.
- Promotes security awareness to the Company computing community.

7.2 System Administrator/Engineers

Any unit maintaining electronic systems, applications, or data is responsible for implementing a level of security consistent with that defined by the Data Custodian. System Administrators/Engineers fill this role.

Note: *System Administrator* can apply to a single person, a group within the unit, or a consultant who acts for the unit.

System Administrators are required to take reasonable action to ensure the authorized use and security of data during storage, transmission, and use. For those systems under its custodianship, the Information Technology Department is responsible for System Administration.

System Administrators:

- Ensure that access to data and applications is secured as defined by the Manager of IT Security and Data Custodian.
- Provide adequate operational controls to ensure data protection.
- Ensure that access requests are authorized.
- Communicate appropriate use, and consequences of misuse, to users who access the systems or data.
- Modify access when employees terminate or transfer.
- Protect sensitive files and access control files from unauthorized activity.
- Secure data transmissions within the controls defined by the Manager of IT Security and Data Custodian.
- Ensure server and workstation integrity through virus protection measures and policies.
- Ensure that server and workstation configurations follow industry best practices, standards and recommendations.

7.3 Network Administrators/Engineers

Network Administrators are required to take reasonable action to ensure the authorized use and security of data during transmission. For those systems under its custodianship, the Information Technology Department is responsible for Network Administration.

- Provide adequate operational controls to ensure data is protected throughout the company WAN, LAN and all other networking technologies.
- Ensure that access to networking equipment and systems are approved by IT Management.
- Communicate appropriate use, and consequences of misuse, to users who access the systems or data.
- Modify access when employees terminate or transfer.

- Protect network devices and access from unauthorized activity.
- Secure data transmissions within the levels defined by the Data Classifications as defined in this policy.
- Ensure network confidentiality, integrity and availability.
- Ensure that network component configurations follow industry best practices, standards and recommendations.

7.4 Internal Audit

Internal auditors are authorized to inquiry-only access to all information and systems and are responsible for assisting Company management in the effective discharge of its duties.

Among their many duties, internal auditors:

- Evaluate Company departments' information security policy and procedures compliance, during operational and administrative audits.
- Evaluate the effectiveness of security procedures and other internal controls.
- Review audit trails provided by System Administrators to determine whether activity is adequately documented.
- Assist management in the investigation of suspected incidents of security breach or improper activity.
- Provide advice regarding internal control relevant to new systems being developed or considered for purchase.

7.5 Enforcement

Any reported abuses of corporate information technologies resources will be investigated. During the investigation, the Company may access the electronic file of the employee. If a computer policy has been violated, disciplinary action may be taken.

The Company will audit resources periodically to ensure that software, use, and computer configurations comply with policy.