# Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Approving Manager</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td></td>
<td>October, 2008</td>
</tr>
<tr>
<td><strong>First MIT Edit</strong></td>
<td></td>
<td>December 6, 2008</td>
</tr>
<tr>
<td><strong>Second MIT Edit</strong></td>
<td></td>
<td>January 12, 2009</td>
</tr>
<tr>
<td><strong>Third MIT Edit</strong></td>
<td></td>
<td>January 21, 2009</td>
</tr>
<tr>
<td><strong>Fourth MIT Edit</strong></td>
<td></td>
<td>March 10, 2009</td>
</tr>
<tr>
<td><strong>Fifth MIT Edit</strong></td>
<td></td>
<td>March 24, 2009</td>
</tr>
<tr>
<td><strong>Release Candidate 1</strong></td>
<td></td>
<td>June 29, 2009</td>
</tr>
<tr>
<td><strong>Release Candidate 2</strong></td>
<td></td>
<td>October 26, 2009</td>
</tr>
<tr>
<td><strong>Version 1.0 – To Be Approved</strong></td>
<td></td>
<td>March 18, 2010</td>
</tr>
<tr>
<td><strong>Version 1.0 – Approved</strong></td>
<td></td>
<td>March 19, 2010</td>
</tr>
</tbody>
</table>

# Approvals

<table>
<thead>
<tr>
<th>Approver</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deborah L. Fisher</td>
<td>Institute Auditor</td>
<td>March 19, 2010</td>
</tr>
<tr>
<td>Israel Ruiz</td>
<td>Vice President for Finance</td>
<td>March 19, 2010</td>
</tr>
<tr>
<td>Marilyn T. Smith</td>
<td>Head of Information Services and technology</td>
<td>March 19, 2010</td>
</tr>
</tbody>
</table>
# Table of Contents

## 1 INTRODUCTION AND SCOPE

1.1 Introduction......................................................................................................................... 6
1.2 What is Payment Card Industry (PCI) Compliance?.............................................................. 6
1.3 Scope of Compliance................................................................................................................ 6
1.4 Scope of Applicability.............................................................................................................. 7

## 2 POLICY ROLES AND RESPONSIBILITIES

2.1 Policy Applicability................................................................................................................ 8
2.2 PCI Executive Committee....................................................................................................... 8
2.3 PCI Security Compliance Officer.......................................................................................... 8
2.4 Information Technology Security Services........................................................................... 8
2.5 Container Administrator......................................................................................................... 9
2.6 System Administrators......................................................................................................... 9
2.7 Merchant Services Team ....................................................................................................... 9
2.8 Merchants............................................................................................................................. 10

## 3 IT CHANGE CONTROL POLICY

## 4 DATA CLASSIFICATION AND CONTROL POLICY

4.1 Policy Applicability................................................................................................................ 12
4.2 Data Access.......................................................................................................................... 12
4.3 Physical Security................................................................................................................... 12
4.4 User Authentication............................................................................................................... 12
  4.4.1 Users............................................................................................................................... 12
  4.4.2 Systems........................................................................................................................ 12
4.5 Account and Access Management......................................................................................... 12
  4.5.1 System Administrator Responsibilities.......................................................................... 12

## 5 DATA RETENTION AND DISPOSAL POLICY

5.1 Policy Applicability................................................................................................................ 14
5.2 Retention Requirements......................................................................................................... 14
5.3 Disposal Requirements......................................................................................................... 15
5.4 Disposal Process.................................................................................................................... 15

## 6 PAPER AND ELECTRONIC MEDIA POLICIES

6.1 Policy Applicability................................................................................................................ 16
6.2 Storage.................................................................................................................................. 16
  6.2.1 Physical Security................................................................................................................. 16
  6.2.1 Hardcopy Media................................................................................................................ 16
  6.2.1 Electronic Media.............................................................................................................. 16
6.3 Destruction............................................................................................................................ 17
7 FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY

7.1 Policy Applicability

7.2 Device Management Responsibilities

7.2.1 Container Administrator

7.2.2 System Administrator

7.2.3 Information Technology Security Services

7.3 Allowed Services

7.4 Allowed Network Connection Paths and Configuration Requirements

7.5 Configuration Review

7.6 Personal Firewalls

8 SYSTEM CONFIGURATION POLICY

8.1 Policy Applicability

8.2 System Build and Deployment

8.2.1 System Purpose

8.2.2 System Configuration Standards

8.2.3 System Configuration Records

8.2.4 System Configuration Process

8.2.5 File Integrity Monitor (FIM) Software

8.2.6 VPN Client and Personal Firewall Software

8.2.7 Anti-virus Software

8.2.8 Network Time Protocol (NTP)

8.2.9 Credit Card Information Processing Application

8.2.10 Credit Card Storage Applications

8.3 Vulnerability Identification and System Updates

8.3.1 Vulnerability Identification

8.3.2 Vulnerability Testing

8.3.3 Security Patch Deployment

8.4 Remote Access

9 ANTI-VIRUS POLICY

9.1 Policy Applicability

9.2 Software Configuration

9.3 Signature Updates

9.4 Software Logging

10 BACKUP POLICY

11 ENCRYPTION POLICY

12 SPECIAL TECHNOLOGIES USAGE POLICY

13 SOFTWARE DEVELOPMENT POLICY

14 INCIDENT RESPONSE PLAN AND PROCEDURES

14.1 Policy Applicability

14.2 Incident Identification

14.3 Reporting and Incident Declaration Procedures

14.4 Incident Severity Classification
1 INTRODUCTION AND SCOPE

1.1 Introduction

This document explains Massachusetts Institute of Technology’s Information security requirements for all employees processing credit cards.

MIT is generally an open community, both physically and from a network perspective. Providing Information Security in such an environment is a significant challenge. Therefore to reduce the probability of a compromise of card holder data at MIT, it is MIT policy to not store card holder data on MIT owned computers. All e-commerce card processing is outsourced.

All merchant e-commerce payment activity is outsourced. When an e-commerce customer is making a purchase from an MIT website, the payment page they see originates from an outsourcing vendor and the payment data they provide does not travel any MIT computer or network.

To facilitate in-person and telephone transactions, MIT personnel may make use of a “Virtual Terminal” application which permits them to access a web site managed by our outsourced provider where they can handle payment and related transactions. MIT requires that PCs used for accessing this “Virtual Terminal” application be managed in a fashion which is compatible with PCI requirements. In particular individual computers must be authorized. Authorized computers will be PCs running the Windows Operating System and joined to a windows “domain” where they are remotely managed in a secure fashion.

1.2 What is Payment Card Industry (PCI) Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding credit card holder information for all credit card brands.

In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version 1.1 of the PCI standard.

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit card holder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites, and retail POS systems that process credit cards over the Internet. This document addresses all the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

1.3 Scope of Compliance

PCI Requirements apply to systems that process card holder data. System components are defined as any network component, server, or application that is included in or connected to the card holder data environment. The card holder data environment is defined as part of the network that possesses card holder data or sensitive authentication data. Because MIT does not permit the storage of card holder data, only the PCs that are used for entry of card holder data to our
outsourced provider(s) are considered in scope. MIT requires our outsourced providers to be PCI compliant and provide MIT with a certificate to that effect.

1.4 Scope of Applicability

Only authorized computers may be used to process card holder data in any fashion. The official list of authorized computers is maintained by the PCI Compliance Officer or their designate.
2 POLICY ROLES AND RESPONSIBILITIES

2.1 Policy Applicability
All employees, contractors, vendors and third-parties that use, maintain or handle MIT merchant card holder data or other data for which PCI Compliance standards are applicable must follow this policy. Policy exemptions will be permitted only if approved in advance and in writing by the PCI Compliance Officer.

2.2 PCI Executive Committee
Responsible for overseeing MIT's PCI Compliance Program. Evaluate PCI policy standards and assess impact to MIT. Review of annual report of merchant operations and PCI status.

2.3 PCI Security Compliance Officer
The PCI Compliance Officer is responsible for coordinating and overseeing Massachusetts Institute of Technology wide compliance with policies and procedures regarding the confidentiality, integrity and security of card holder data and other data that must be managed in compliance with the PCI Data Security Standards.

The PCI Compliance Officer works closely with the IT Managers and other Massachusetts Institute of Technology managers and staff involved in securing card holder data to enforce established policies, identify areas of concern, and implement appropriate changes as needed. Specific responsibilities of the PCI Compliance Officer include:

- Make high-level decisions pertaining to the information security policies and their content. Approve, in advance, exceptions to these policies on a case-by-case basis.
- On an annual basis, coordinate a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- Annually review the MIT PCI Security policies and procedures to maintain adequacy in light of emergent business requirements or security threats.
- Make sure third parties with whom card holder data is shared are required to adhere to the PCI DSS requirements and to acknowledge they are responsible for the security of the card holder data which they possess.
- Create new information security policies and procedures when need arise. Maintain and update existing information security policies and procedures. Review the policy on an annual basis and assist management with the approval process.

2.4 Information Technology Security Services
Successfully securing MIT information systems requires that the various departments and groups consistently adhere to a shared vision for security.

Although individual departments are responsible for information security, MIT has a central Information Technology Security Services (ITSS) team. ITSS is part of the Information Services and Technology (IS&T) department. IS&T is MIT’s central Information Technology department.

ITSS also is the first line of contact for reports of security incidents. It maintains a problem tracking system which tracks issues. When a department owned system is involved, ITSS works with the staff in the department to help resolve any security issues.
The Information Technology Security Services team is dedicated to security education and awareness. Specific responsibilities of ITSS include:

- Review logs daily, follow up on any exceptions identified.
- Act as a central coordinating department for tracking of the Information Security incidents.
- Create, maintain and distribute incident response and escalation procedures.
- Monitor and analyze security alerts and distribute information to appropriate information security, technical and business unit management personnel.

2.5 Container Administrator

All MIT systems that handle card holder Data will be part of a Windows Managed domain (or equivalent). Each domain that handles card holder Data will have a special restricted set of "Container Policies." The Container Administrator is responsible for ensuring that these policies provide both for over-all security as well as compliance with PCI Security Standards and this Policy document.

2.6 System Administrators

Each computer system at MIT that handles card holder Data will have at least one System Administrator responsible for it.

MIT System Administrators are the direct link between information security policies and the network, systems and data. System Administrator responsibilities include:

- Applying MIT information security policies and procedures as applicable to all information assets including ensuring that systems that handle card holder data are compliant with appropriate PCI standards.
- Administering user account and authentication management.
- Ensure that all systems have appropriate security updates installed and appropriate anti-virus and anti-spyware.
- All systems that handle card holder data are properly joined to the appropriate restricted "windows Container" or equivalent.

2.7 Merchant Services Team

The MIT Merchant Services Team has an important role with regards to MIT information security. The following items are the ongoing responsibility of the Merchant Services Team:

- Publish and disseminate MIT information security policies and acceptable use guidance as they apply to credit card processing, to all relevant credit card merchants and users.
- Background checks are not performed at MIT, as Merchants and anyone at MIT processing credit cards do not have access to card holder data and only have access to one credit card number at a time.
- Work with ITSS on disseminating security awareness information to system users utilizing multiple methods of communicating awareness and educating employees (for example, posters, letters, emails, meetings, etc).
- Is notified of terminated employee's and arranges for the terminated employee's access to any card holder information or systems to be removed.

---

1A “Container” is a Microsoft technical term denoting a set of systems that have an enforced common set of policies such as firewall rules, access rules, etc.
2.8 Merchants
Each Merchant that is processing credit cards that uses MIT computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all MIT merchants:

- Understand what the consequences of their actions are with regard to computing security practices and act accordingly. Embrace the "Security is everyone’s responsibility" philosophy to assist MIT in meeting its business goals.
- Maintain awareness of the contents of the information security policies.
- Classify confidential and sensitive information that is received unclassified. Limit the distribution of this information accordingly.
3 IT CHANGE CONTROL POLICY

MIT does not develop applications or manage systems that store card holder data. As such there are no systems to exercise change management over. Card holder data is passed through merchant PCs (via a web browser) when data is entered into the Cybersource “Virtual terminal” web based application. These PCs are remotely managed and monitored, as described elsewhere in this document.
4 DATA CLASSIFICATION AND CONTROL POLICY

4.1 Policy Applicability
All card holder data stored and accessed on MIT information systems, whether managed by employees or by a third party, must follow this policy.

4.2 Data Access
No card holder data is stored on MIT computers. We therefore have no data access policy for card holder data.

4.3 Physical Security
MIT does not store credit card data, and uses a 3rd party provider to host all credit card processing, transmitting and storage of data.

4.4 User Authentication

4.4.1 Users
Each user’s access privileges shall be authorized according to business need. User access authority to computer resources shall be provided only when necessary to perform tasks related to MIT’s business.

The use of non-authenticated (e.g. no password) User IDs or User IDs not associated with a single identified user are prohibited.

4.4.2 Systems
Each computer system shall have an automated or procedural access control process to authenticate all system users. The process must:

- Identify each User through a unique User identifier (user ID).
- If the chosen user ID is already being used, the most logical id will be assigned
- Authenticate every user ID, system account and application account with a password.
- Require that new passwords cannot be the same as the 3 previously used passwords.

4.5 Account and Access Management

4.5.1 System Administrator Responsibilities
The System Administrator has the following responsibilities regarding user account and access management:

- Account creation requests must specify access either explicitly or via a “role” that has been mapped to the required access.
- Passwords set by System Administrators must be changed by the user immediately upon the users’ next login. System Administrators must set initial passwords that are unique and compliant with the password rules.
- System Administrators must validate the identity of users before performing a password reset. The approved means for validating identity at MIT is by doing it in person with a valid
employee ID, or remotely by providing uniquely identifying pieces of information. Examples could include: employee ID, full name.

- Vendor accounts used for remote maintenance must only be enabled during the time that access is needed and monitored while being used.
5 DATA RETENTION AND DISPOSAL POLICY

5.1 Policy Applicability
All data deemed confidential or sensitive must follow this policy.

5.2 Retention Requirements
All confidential and sensitive data, regardless of storage location, will be retained only as long as required for legal, regulatory and business requirements. The specific retention length will be established by the data creator.

As a special case, card holder data used for single transactions may be kept for up to 120 days. This applies for card holder data retained in any kind of format including digital and paper.

card holder data utilized for recurring transactions will be retained by our third party outsourcing agent. MIT will not retain card holder data in electronic form on MIT information processing systems.

All system audit logs related to PCI Compliance must be retained for one year with 90 days available for online viewing.
5.3 Disposal Requirements
All confidential or sensitive electronic data, when no longer needed for legal, regulatory or business requirements must be removed from MIT systems using an approved method documented in this policy. See the Paper and Electronic Media Policies (Section 6) for more details. This requirement includes all data stored in systems, temporary files or contained on storage media.

All confidential or sensitive hardcopy data, when no longer needed for legal, regulatory or business requirements must be disposed by using an approved method documented in this policy. See the Paper and Electronic Media Policies (Section 6) for more details.

5.4 Disposal Process
A programmatic (automatic) process will be executed on card holder information systems nightly to remove all confidential or sensitive data that exceeds business retention requirements.

Other applicable data stored in files and directories where the containing media will be re-used must be deleted securely by a “wiping” utility.

Media containing confidential or sensitive card holder data that should no longer be retained must be disposed of in a secure and safe manner.

● Before computer or communications equipment can be sent to a vendor for trade-in, servicing or disposal, all confidential or sensitive information must be destroyed or removed.

Outsourced destruction of media containing confidential or sensitive information must use a bonded Disposal Vendor that provides a “Certificate of Destruction”.
6 PAPER AND ELECTRONIC MEDIA POLICIES

6.1 Policy Applicability
All employees handling hardcopy or electronic media must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the PCI Compliance Officer.

6.2 Storage

6.2.1 Physical Security
Hard copy materials and electronic media containing confidential or sensitive information must be protected by appropriate physical access controls.

- Appropriate facility controls must be used to limit and monitor physical access to systems that store confidential or sensitive card holder data.²

6.2.1 Hardcopy Media
Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

- At no time are printed reports containing confidential or sensitive information to be removed from any MIT secure office environment.
- Printed reports containing consumer confidential or sensitive data are to be physically retained, stored or archived only within secure MIT office environments, and only for the minimum time deemed necessary for their use.
- All hardcopy material containing confidential or sensitive information should be clearly labeled as such.
- All confidential or sensitive hardcopy media must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin).
- Confidential or sensitive hardcopy material is never to be stored in unlocked or insecure containers or open workspaces.

6.2.1 Electronic Media
Electronic media containing confidential or sensitive information (e.g., CD, DVD, floppy disk, hard disk, tape, etc.) is subject to the following storage guidelines:

- At no time is electronic media containing confidential or sensitive card holder data be removed from any MIT secure office environment with the exception of computer system backups.
- Electronic media containing card holder confidential or sensitive data are to be physically retained, stored or archived only within secure MIT office environments, and only for the minimum time deemed necessary for their use.
- All electronic media containing confidential or sensitive information should be clearly labeled as such.
- All removable, confidential or sensitive electronic media must be stored securely.
- All media must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked.

²Note: PCI Requirements 9.1-9.4 are exclusions for MIT (see Guidance for Exclusions of Certain, Specific Requirements). MIT does not plan to store media nor have systems that contain card holder data.
6.3 Destruction
All hardcopy shred bins must remain locked at all times (until shredding). Employees should make every effort to immediately cross-cut shred any printed material containing confidential or sensitive information.
7 FIREWALL AND ROUTER SECURITY ADMINISTRATION
POLICY

7.1 Policy Applicability
This policy applies to firewalls used to protect computers that process card holder data.

7.2 Device Management Responsibilities
MIT uses software firewalls on individual computers that process card holder data. The configuration of this firewall is centrally managed and reviewed by the PCI Compliance Officer or designate.

7.2.1 Container Administrator
- Assure that changes to firewall hardware or software or security rules are approved by PCI Compliance Officer and follow all change control policies and procedures.
- Document all firewall security rule changes.
- Enable appropriate logging on all security systems and perform active daily monitoring of the logs that report security events.
- Report network security incidents to ITSS immediately upon discovery.
- Coordinate an appropriate response with ITSS to mitigate security events.

7.2.2 System Administrator
All configuration of systems that process card holder data are derived from a common repository (a “Windows Container” or equivalent). The System Administrator is responsible for ensuring that systems are properly setup to receive their configuration from the appropriate location. The System Administrator should also act as a backup to the Container Administrator by ensuring that PCs under their control are in fact properly configured.

7.2.3 Information Technology Security Services
The Information Technology Security Services Team (ITSS) will provide advice as requested and needed to aid in the configuration of security software, including firewalls, on computers handling card holder data.

7.3 Allowed Services
No incoming services are permitted on computers that handle card holder data.

7.4 Allowed Network Connection Paths and Configuration Requirements
All computers that handle card holder data operate a “personal firewall” such that the network they are connected to is out of scope for PCI Compliance.

7.5 Configuration Review
Quarterly Configuration review of the computers that handle card holder data is handled by the Container Administrator with assistance from System Administers.
7.6 Personal Firewalls

All computers that handle card holder data run a personal firewall that is centrally managed.
8 SYSTEM CONFIGURATION POLICY

8.1 Policy Applicability
This policy applies to all computers that may access or process card holder data.

8.2 System Build and Deployment

8.2.1 System Purpose
MIT does not store or directly process card holder data. However MIT systems (aka Merchant PCs) are used as virtual terminal devices for data entry of card holder data. As such this section applies to the configuration of those PCs.

8.2.2 System Configuration Standards
Merchant PCs will be configured to be part of a Windows Domain (or equivalent). The domain configuration will be setup to be compliant with this document.

8.2.3 System Configuration Records
The Container Administrator maintains the documentation about the configuration that is deployed to Merchant PCs.

8.2.4 System Configuration Process
The Container Administrator is responsible for the maintenance of the container configuration. Proposed changes will be reviewed with the PCI Compliance Officer.

8.2.5 File Integrity Monitor (FIM) Software
For systems storing or processing confidential or sensitive information deploy file integrity monitoring (FIM) software to alert personnel to unauthorized modification of critical system or content files. Configure FIM to perform critical file comparisons at least weekly.

8.2.6 VPN Client and Personal Firewall Software
All computers that handle card holder data do not accept incoming connections.

8.2.7 Anti-virus Software
All servers, workstations, and laptops utilizing an operating system commonly affected by viruses must have anti-virus software installed as described in the Anti-virus Policy (Section 9).

8.2.8 Network Time Protocol (NTP)
MIT operates a network of NTP servers. This includes at least two Stratum I servers with GPS or WWV synchronized clocks. NTP is then distributed around campus by a network of Stratum 2 servers. Individual computers may be synchronized to this time distribution network. Computers that provide timestamps for transactions or log entries should be synchronized with NTP.

8.2.9 Credit Card Information Processing Application
MIT uses a 3rd party vendor and uses tokens for all credit cards processed. The application does not pass credit card data.
8.2.10 Credit Card Storage Applications
MIT does not store card holder data on MIT systems.

8.3 Vulnerability Identification and System Updates

8.3.1 Vulnerability Identification
The Information Technology Security Services Team tracks vulnerabilities and threats to MIT’s IT infrastructure in cooperation with the Operations and Infrastructure Services organization.

The primary method for identifying new threats as they arise will be through vendor and security specific Internet mailing lists. Although not complete, the following lists should be subscribed to as well as other vendor lists applicable to MIT specific software packages and systems:

- CERT
- NT BUGTRAQ
- SANS

MIT also has world renowned security experts on its staff who maintain communications with peers at other institutions. This often results in MIT having early access to critical vulnerability information.

8.3.2 Vulnerability Testing
The Information Technology Security Services Team will periodically scan systems at MIT to verify that they are not vulnerable to attacks. This is also done on an ad-hoc basis when new threats surface in the community.

In addition MIT has contracted with a external PCI scanning vendor to perform monthly scans of Merchant PCs.

Once per year MIT will perform an internal penetration test of 10% of the authorized merchant PCs.

8.3.3 Security Patch Deployment
MIT maintains an active security patch system, including our own Microsoft SUS service. Patches will be pushed out to systems that handle card holder data. Patches will be made available as soon as they are verified to not cause system difficulties (for critical security updates this is often done within a few hours).

8.4 Remote Access
Computers handling card holder data may not be accessed remotely.
9 ANTI-VIRUS POLICY

9.1 Policy Applicability
This policy applies to systems that handle card holder data.

9.2 Software Configuration
All systems that handle card holder data are centrally managed. All systems are configured with McAfee Anti-Virus and Anti-Malware software.

9.3 Signature Updates
All systems with anti-virus software must be configured to update virus signatures and scan engines on at least a daily basis.

9.4 Software Logging
All systems that handle card holder data log anomalies to a central location and reviewed on a daily basis. Centralized log monitoring will be performed by ITSS.
10 BACKUP POLICY

All computers that handle card holder data are “dataless” in the sense that they do not store card holder data or other transactional information. In essence they are run as “virtual terminals” to our third party outsourcing provider. As such there is no requirement on backups. However they will be maintained in a way that will permit them to be re-imaged/re-created in the event of computer or component failure.

All data storage of card holder data is performed by a third party provider who is required by to PCI compliant which includes an appropriate backup policy.
11 ENCRYPTION POLICY

MIT does not store card holder data, so no encryption policy is required. All information transmitted via computers that handle card holder data will be done using standard web browsers making use of standard SSL ciphers.

All data storage of card holder data is performed by a third party provider who is required by to PCI compliant which includes an appropriate encryption policy.

It is against MIT policy to transmit card holder data electronically with the exception of the use of the “virtual terminal” website to interact with our third party processor.
12 SPECIAL TECHNOLOGIES USAGE POLICY

MIT does not have a special use technology policy as we do not store card holder data and all computers that process card holder data do not permit incoming connections.
13 SOFTWARE DEVELOPMENT POLICY

MIT does not develop software that processes or handles card holder data in any way.
14 INCIDENT RESPONSE PLAN AND PROCEDURES

14.1 Policy Applicability
All incident detections and responses, especially related to critical systems, must follow this policy.

14.2 Incident Identification
Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records
- Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals)
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, and physical security alarms)

All employees, regardless of job responsibilities, should be aware of the potential incident identifiers and who to notify in these situations. In all cases, every employee should report incidents per the instructions under 14.3 Incident Reporting, unless they are assigned other activities within the incident response plan.

14.3 Reporting and Incident Declaration Procedures
The Information Protection Team (InfoProtect) should be notified immediately of any suspected or real security incidents involving MIT computing assets, particularly any critical system or system that handles or processes card holder or other Personally Identifiable Information (PII). If it is unclear as to whether a situation should be considered a security incident, the Information Technology Security Services Team (ITSS) should be contacted to evaluate the situation.

With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by trained personnel or under the oversight of trained personnel, to assure the integrity of the incident investigation and recovery process. When faced with a potential situation you should do the following,

- If the incident involves a compromised computer system.
  - Do not alter the state of the computer system.
  - The computer system should remain on and all currently running computer programs left as is. Do not shutdown the computer or restart the computer.
  - Immediately disconnect the computer from the network by removing the network cable from the back of the computer.

- Report the security incident.
  - Contact the Information Technology Security Services Team to report any suspected or actual incidents. The Information Technology Security Services Team (ITSS) can be reached by sending e-mail to security@mit.edu. Off hours emergency situations can be
handled by paging the NIST On-Call person at x3-8400 (617-253-8400) and follow the voice prompts. Someone will be paged.

- No one should communicate with anyone outside of their supervisor(s) or appropriate authorized individuals about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Office of the General Counsel (OGC).
- Document any information you know while waiting for the Information Technology Security Services Team to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

14.4 Incident Severity Classification

The Information Technology Security Services Team will first attempt to determine if the security incident justifies a formal incident response.

In cases where a security incident does not require an incident response the situation will be forwarded to the appropriate area of IT to ensure that all technology support services required are rendered.

The following descriptions should be used to determine what response the Information Technology Security Services Team will take.

- **Level 1** - One instance of potentially unfriendly activity (e.g., finger, unauthorized telnet, port scan, corrected virus detection, unexpected performance peak, etc.).

- **Level 2** - One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer successful virus infection on a non-critical system, unauthorized vulnerability scan, etc.) or a second Level 1 attack.

- **Level 3** - Serious attempt or actual breach of security (e.g., multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful buffer/stack overflow, successful unauthorized access to sensitive or critical data or systems, broken lock, stolen papers, etc.) or a second Level 2 attack.

Any Level 1 type incident occurring against systems storing confidential or sensitive data or originating from unauthorized internal systems is classified as a Level 2.

14.5 Incident Response

14.5.1 Typical Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls. The following actions should be taken by the Information Technology Security Services Team once an incident has been identified and classified.

14.5.1.1 Level 1

Contain and Monitor

1. If possible, record the user, IP address and domain of intruder.

2. Utilize approved technology controls to temporarily or permanently block the intruder’s access.
3. Maintain vigilance for future break-in attempts from this user or IP address.

14.5.1.2 Level 2
Contain, Monitor and Warn
1. Collect and protect information associated with the intrusion.
2. Utilize approved technology controls to temporarily or permanently block the intruder’s access.
3. Research the origin of the connection.
4. Research potential risks related to intrusion method attempted and re-evaluate for higher classification and incident containment, eradication, and recovery as described for Level 3 incident classifications.

14.5.1.3 Level 3
Contain, Eradicate, Recover and perform Root Cause Analysis
1. If the incident involved credit card systems the Acquirer and applicable card associations must be notified. See the Credit Card Compromise – Special Response (Section 14.5.2) for more details.
2. Contain the intrusion and decide what action to take. Consider unplugging the network cables, applying highly restrictive ACLs, deactivating or isolating the switch port, deactivating the userID, terminating the user’s session/change password etc.
3. Collect and protect information associated with the intrusion via offline methods. In the event that forensic investigation is required the Information Technology Security Services Team will work with legal and management to identify appropriate forensic specialists.
4. Notify management of the situation and maintain notification of progress at each following step.
5. Eliminate the intruder’s means of access and any related vulnerabilities.
6. Research the origin of the connection.
7. Research potential risks related to or damage caused by intrusion method used.

14.5.2 Credit Card Compromise – Special Response
For any incidents involving potential compromises of credit card information, the Information Technology Security Services Team will use the following procedure:
1. Contain and limit the exposure. Conduct a thorough investigation of the suspected or confirmed loss or theft of account information. To facilitate the investigation:
   a. Log all actions taken (e.g., bound notebook, video camera, etc).
   b. Utilize chain of custody techniques during all transfers of equipment and information related to the incident.
   c. Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
   d. Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the network cable, deactivate switch port, isolate to contained environment e.g. isolated VLAN). To preserve the evidence for a forensic investigation it is extremely important to not access the system. Use the Critical Systems Restore Strategy (Section 14.8) to reestablish critical business functions.
2. Preserve logs and electronic evidence.
   a. Be on high alert and monitor all card holder information systems.

3. Alert all necessary parties. Be sure to notify:
   a. Information Technology Security Services (ITSS), if they are not already involved

4. ITSS will work with the Office of the General Counsel and the PCI Compliance Officer to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)

Follow appropriate procedures for each card association which MIT utilizes for credit card services.

*Note: The information below is considered accurate as of the publication of this document. However ITSS in concert with the PCI Compliance Officer and will maintain up-to-date copies.*

**Visa**

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at:


**MasterCard**


**American Express**

Contact your relationship manager or call the support line at 1-(800)-528-4800 for further guidance.

**Discover Card**

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm

**14.5.3 Root Cause Analysis and Lessons Learned**

Not more than one week following the incident, members of the Information Technology Security Services Team and all affected parties will meet to review the results of the investigation conducted under step 1, section 14.5.2 of this document to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly. Upon conclusion of the investigation, systems will be restored to their non compromised state.
14.6 Plan Testing and Training
At least once a year, a mock-incident will be initiated to facilitate testing of the current plan. The exact incident to be tested will be at the discretion of the Information Technology Security Services Team. Once complete, a follow-up session, as detailed above in section 14.5.3, will be held.

All MIT employees that could have an active role within incident response will be part of the test process.

Training regarding incident response responsibilities must be performed regularly to ensure employee’s readiness for test and actual incidents.

14.7 Automated Security System Notifications
All automated intrusion detection systems within the MIT environment, including intrusion detection sensors and file integrity checking systems, will be configured to automatically notify the Information Technology Security Services Team of any potential compromises or attacks.
15 LOGGING CONTROLS POLICY

MIT stores no card holder data. Those systems that are used to process card holder data as “virtual terminals” will have their logs recorded in a central location.

15.1 Log Security

All event logs must be collected in a centralized location or media that is difficult to alter and protected from unauthorized access. The viewing of such logs is to occur on a need only basis. Summaries of the logged information and any anomalies will be sent via e-mail daily to appropriate system and container administrators.
16 RESPONSIBILITIES AS A SERVICE PROVIDER

MIT is not a service provider.
This section defines the scope of the Payment Card Industry Data Security Standards (PCI DSS) within MIT network environment. All the policies and procedures within this document must be followed within the card holder environment to maintain compliance with the PCI DSS. Any deviation may put MIT in a dangerous position by weakening the security posture of the different systems and making the organization liable to fines.

16.1 A.1 Description of card holder Environment

Card holder data is entered into MIT’s network environment via the following channels: e-commerce, telephone, mail orders, fax, and Point of Sales (POS). All e-commerce applications redirect their payment page to an outsourced PCI compliant third party processor (Cybersource). Card holder data received via a call center, mail order, fax or at Point of Sale are entered into a “virtual terminal” which is a PC which is running Windows and jointed to the MIT “win.mit.edu” domain and placed in a special Windows "Container” that enforces security policies to reduce or eliminate the chance for system compromise to reveal card holder data. No card holder data is retained in electronic form on the MIT campus.
This page is intentionally blank to indicate the end of this document.