



# **MICROS Systems, Inc. Enterprise Information Security Policy and Standards**

Revision 6.0

**March, 2009**

## Table of Contents

### Information Security Policies:

<b>1. Information Security Organization Policy.....</b>	<b>6</b>
<b>2. Access Management Policy.....</b>	<b>7</b>
<b>3. Systems Security Policy.....</b>	<b>8</b>
<b>4. Network Security Policy.....</b>	<b>9</b>
<b>5. Application Security Policy.....</b>	<b>10</b>
<b>6. Data Security/Management Policy.....</b>	<b>11-12</b>
<b>7. Security Incident Handling Policy.....</b>	<b>13</b>
<b>8. Security Operations Policy.....</b>	<b>14</b>
<b>9. Personal Information Protection Policy.....</b>	<b>15</b>
<b>10. Medical Information Privacy Policy.....</b>	<b>16</b>
<b>11. Relation to MICROS Systems, Inc. Policies.....</b>	<b>17</b>
<b>12. Interpretation.....</b>	<b>17</b>

**13. Violations.....17**

**14. Enforcement.....17**

**15. Ownership.....17**

**16. Revisions.....17**

**Information Security Standards:**

**1. Information Security Organization Standard.....18**

**2. Authentication And Password Standard.....19-20**

**3. Authentication Administration Standard.....21-23**

**4. Third-Party Access Standard.....24-26**

**5. Malware Protection Standard.....27-30**

**6. System Audit Logging Standard.....31-33**

**7. Host Security Standard.....34-36**

**8. Laptop Security Standard.....37-38**

<b>9. Software Security Patching Standard.....</b>	<b>39-40</b>
<b>10. System Hardening Standard.....</b>	<b>41-42</b>
<b>11. DMZ Server Security Standard.....</b>	<b>43-45</b>
<b>12. Network Security Standard.....</b>	<b>46-47</b>
<b>13. Wireless Communication Standard.....</b>	<b>48-50</b>
<b>14. Firewall Standard.....</b>	<b>51-52</b>
<b>15. Remote Access Standard.....</b>	<b>53-55</b>
<b>16. Application Security Standard.....</b>	<b>56-57</b>
<b>17. Database Security Control Standard.....</b>	<b>58-59</b>
<b>18. Data Backup And Recovery Standard.....</b>	<b>60</b>
<b>19. Encryption Standard.....</b>	<b>61-62</b>
<b>20. Security Incident Response Team.....</b>	<b>63-64</b>
<b>21. Information Security Assessment Standard.....</b>	<b>65-67</b>

**22. System Operation Acceptance Standard.....68-69**

**23. Information Security Operations Standard.....70-71**

**24. Personal Information Protection Standard.....72-74**

**25. Medical Information Privacy Standard.....75-81**



## **1. INFORMATION SECURITY ORGANIZATION POLICY (MEIS-001)**

### **1.1 PURPOSE**

This policy describes the MICROS Systems, Inc. Information Security department and how their management framework promotes and manages the performance of information security throughout corporation and its business units.

### **1.2 SCOPE**

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or managed by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **1.3 DEFINITIONS**

None

### **1.4 STATEMENT OF POLICY**

Appropriate organizational capability shall be maintained to create, promote and manage the Information Security policies to support data privacy compliance, industry regulatory compliance, network security, security operations, security incident handling and security awareness.

### **1.5 REFERENCE**

**-MEIS-001.001                      Information Security Organization Standard**



## **2. ACCESS MANAGEMENT POLICY (MEIS-002)**

### **2.1 PURPOSE**

The purpose of this policy is to ensure appropriate mechanisms, based on business and legal requirements, are provided for the control, administration, and tracking of access to and use of MICROS Systems, Inc. business systems and company information, and for the protection from unauthorized or unapproved activity relating to, or destruction of, such systems and information.

### **2.2 SCOPE**

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **2.3 DEFINITIONS**

None

### **2.4 STATEMENT OF POLICY**

Access to and use of information and business resources shall be controlled and administered based on defined business and legal requirements.

### **2.5 REFERENCE**

- |                      |   |
|----------------------|---|
| <b>-MEIS-002.001</b> | <b>Authentication &amp; Password Standard</b> |
| <b>-MEIS-002.002</b> | <b>Authentication Administration Standard</b> |
| <b>-MEIS-002.003</b> | <b>Third Party Access Standard</b>            |



### **3. SYSTEMS SECURITY POLICY (MEIS-003)**

#### **3.1 PURPOSE**

The purpose of this policy is to establish standards for the security of host equipment that is owned and/or operated by MICROS Systems, Inc... These standards are designed to minimize the potential exposure to the corporation from damages which may result from the unauthorized use of company owned or managed resources. Damages include, for example, the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, etc..

#### **3.2 SCOPE**

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

#### **3.3 DEFINITIONS**

**Host** -A Host is defined as any MICROS Systems, Inc. owned or managed computer.

#### **3.4 STATEMENT OF POLICY**

All computers owned and/or operated should be securely configured in accordance with its intended use.

#### **3.5 REFERENCE**

- MEIS-003.001 Malware Protection Standard**
- MEIS-003.002 System Audit Logging Standard**
- MEIS-003.003 Host Security Standard**
- MEIS-003.004 Laptop Security Standard**
- MEIS-003.005 Software Security Patching Standard**
- MEIS-003.006 System Hardening Standard**
- MEIS-003.007 DMZ Server Security Standard**



## **4. NETWORK SECURITY POLICY (MEIS-004)**

### **4.1 PURPOSE**

This purpose of this policy is to describe network security to prevent network client workstations from accessing or using services outside of those they are authorized to use or access by implementing controls such as firewalls or segmentation at strategic points of the network.

### **4.2 SCOPE**

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **4.3 DEFINITIONS**

**Computing Resource** -any physical or virtual component of limited availability within a computer system or network. Every internal and external device connected to a computer system is a resource including files, network connections and memory areas.

### **4.4 STATEMENT OF POLICY**

Network designs and processes must be utilized to restrict the path between network client workstations and MICROS Systems, Inc. computing resources to minimize opportunities for unauthorized use or access.

### **4.5 REFERENCE**

<b>-MEIS-004.001</b>	<b>Network Security Standard</b>
<b>-MEIS-004.002</b>	<b>Wireless Security Standard</b>
<b>-MEIS-004.003</b>	<b>Firewall Standard</b>
<b>-MEIS-004.004</b>	<b>Remote Access Standard</b>



## **5. APPLICATION SECURITY POLICY (MEIS-005)**

### **5.1 PURPOSE**

This policy requires the integration of appropriate security controls and audit capabilities during the systems life cycle process.

### **5.2 SCOPE**

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **5.3 DEFINITIONS**

Systems life cycle process -a conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed system.

### **5.4 STATEMENT OF POLICY**

Software development or implementation life cycle for purchased or internally developed applications must include appropriate security controls and audit capabilities to prevent the loss, modification, corruption or misuse of company information technology assets.

### **5.5 REFERENCE**

- |                      |   |
|----------------------|---|
| <b>-MEIS-005.001</b> | <b>Application Security Standard</b>      |
| <b>-MEIS-005.002</b> | <b>Database Security Control Standard</b> |



## **6. DATA SECURITY/MANAGEMENT POLICY (MEIS-006)**

### **6.1 PURPOSE**

This policy requires that data security be implemented to properly secure company information and business systems of MICROS Systems, Inc., and prevent their loss, modification, corruption or misuse by leveraging sufficient data backup and recovery, encryption or similar security measures, and secure data transport.

### **6.2 SCOPE**

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **6.3 DEFINITIONS**

**Company Information** -Material non-public information, confidential information, personally identifying information, and legally privileged information.

**Business Systems** – Include, but are not limited to, mainframe computers and terminals, distributed servers, communication equipment, personal computers (i.e., desktops, laptops), storage and printing devices, handheld devices (i.e., blackberry, PDAs) electronic mail, telephones, facsimile machines, voice mail, toll free communications and Internet access.

**Information Security** – Preservation of the confidentiality, integrity and availability of information.

**Confidentiality** – Ensuring that information is accessible only to those authorized to have access.

**Integrity** – Safeguarding the accuracy and completeness of information and processing methods .

**Availability** – Ensuring that authorized users have access to the information and associated assets when required.

## **6.4 STATEMENT OF POLICY**

The confidentiality, integrity and availability of information assets must be protected according to data classification and applicable law when being handled and/or transmitted.

## **6.5 REFERENCE**

-MEIS-006.001  
-MEIS-006.002

Data Backup/Recovery Standard  
Encryption Standard  
PCI Data Security Standard (PCI-DSS)



## **7. SECURITY INCIDENT HANDLING POLICY (MEIS-007)**

### **7.1 PURPOSE**

This policy defines and describes how incidents relating to the overall security, and more specifically the confidentiality, integrity and availability of MICROS Systems, Inc. information must be managed, escalated and reported to the appropriate stakeholders.

### **7.2 SCOPE**

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **7.3 DEFINITIONS**

Security-related incident – Any event and/or condition resulting from intentional or unintentional actions that has the potential to impact the confidentiality, integrity, or availability of a business system or the security of a physical facility.

### **7.4 STATEMENT OF POLICY**

All employees and contractors are responsible for reporting any security related incidents they may become aware of by utilizing the company's incident response process.

### **7.5 REFERENCE**

-MEIS-007.001                      SIRT Standard



## 8. SECURITY OPERATIONS POLICY (MEIS-008)

### 8.1 PURPOSE

The purpose of this policy is to establish standards for the secure operation and administration of business systems that are owned and/or operated by MICROS Systems, Inc. These standards are designed to minimize the potential exposure to MICROS Systems, Inc. from damages which may result from improper operation and administration of company owned and/or managed resources. Damages include, for example, the loss of sensitive or company confidential data, intellectual property, damage to public image, and damage to critical internal systems.

### 8.2 SCOPE

This policy applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 8.3 DEFINITIONS

**Compromise** – Intrusion into business systems where unauthorized access, disclosure, modification, or destruction of data is confirmed.

**Security Incident** – Any event and/or condition resulting from intentional or unintentional actions that has the potential to impact the confidentiality, integrity, or availability of a business system or the security of a physical facility.

### 8.4 STATEMENT OF POLICY

All computer processing and information assets owned or leased by the company should be operated by persons with defined roles and responsibilities and administered using documented procedures in a manner that is both efficient and effective in protecting the company's information security.

### 8.5 REFERENCE

-MEIS-008.001	Information Security Assessment Standard
-MEIS-008.002	System Operational Acceptance Standard
-MEIS-008.003	Information Security Administration Standard





## **11. RELATION TO MICROS SYSTEMS, INC. POLICIES**

If there is any conflict between these policies and standards, and any MICROS Systems, Inc. company policy, including but not limited to, Legal policy, Ethics or Code-of-Conduct policy and/or Human Resources or Employee policy, collectively referred to as “Company Policy”, the terms of the Company Policy shall govern.

## **12. INTERPRETATION**

All questions pertaining to this policy should be directed to the Chief Security Officer or it’s designate. In the event that this policy cannot be executed for a specific situation, a statement of risk along with compensating controls to adhere to this standard shall be presented to the Chief Security Officer, or designate, for review and acceptance. The Chief Security Officer, or designate, has the ability to provide a variance to the policy based on the statement of risk.

## **13. VIOLATIONS**

Any violations of this standard may result in disciplinary action, up to and including termination of employment. This document in no way shall be construed to represent a contract of employment between MICROS Systems, Inc. and any employee or third party.

Any employee or third party, who is requested to undertake an activity which he or she believes is in violation of this standard, should provide a written or verbal complaint to his or her manager, or any manager in the Human Resources department as soon as possible.

## **14. ENFORCEMENT**

If there is a discovery of violation to this policy, the Chief Security Officer or its designate shall be notified as soon as possible.

## **15. OWNERSHIP**

This policy is owned by the Chief Security Officer. It is the responsibility of the Information Security department to review this policy on an annual basis.

## **16. REVISIONS**

Within the constraints of applicable law, MICROS Systems, Inc. reserves the right to modify or terminate this policy or standard at any time it deems necessary, with or without notice. In the event that a standard cannot be executed for a specific situation, a statement of risk along with compensating controls to adhere to the standard will be presented to the Chief Security Officer, or it’s designate, for review and acceptance. The Chief Security Officer, or designate, has the ability to provide a variance to a standard based on the statement of risk.



## **Information Security Organization Standard MEIS-001.001**

---

### **1. PURPOSE**

This standard defines and describes the guidance to be provided on the overall roles and responsibilities within the Information Security department, for implementing the necessary controls.

### **2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **3. DEFINITIONS**

None

### **4. STATEMENT OF STANDARD**

The Information Security department, in coordination with the M.I.S., H.R, Legal and such other functional departments or qualified third parties as may be necessary and appropriate, shall:

- a. Be responsible for promoting awareness and facilitating training on the Company's information security policies and standards;
- b. Ascertain, review and implement proper compliance with legal, auditing, regulatory, industry and contractual requirements;
- c. Establish communication which reaches all appropriate levels of the company;
- d. Facilitate the performance of independent reviews to provide assurances that the organizational practices properly reflect applicable security policies and standards.
- e. Establish a process to identify newly discovered security vulnerabilities and update standards to address new vulnerability issues;
- f. Require that all employees and contractors shall acknowledge in writing that they have read and understand the company's security policies and procedures.



**1. PURPOSE**

The purpose of this standard is to establish the rules for authentication and password specifications for MICROS Systems, Inc. information resources and support services.

**2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

**3. DEFINITIONS**

Password – An authentication factor that the user memorizes and that is managed by a device, software or an individual; a password authenticates a person by using something the person knows (i.e., a secret word or code).

**4. STATEMENT OF STANDARD**

- a. Blank passwords are prohibited and shall never be used.
- b. Passwords shall be a minimum length of eight (8) characters and at least three of the following character types:
  - i. Alphabetic-Lower Case
  - ii. Alphabetic-Upper Case
  - iii. Numeric
  - iv. Special character (!,\$,#,%)
- c. Passwords shall not be the same as the User Name or User ID.
- d. Users shall be required to change their passwords at least once every ninety days.
- e. The six most recent passwords shall not be used when selecting a new password.
- f. Passwords shall not be embedded in applications or program source code.
- g. Users shall maintain password and PIN secrecy at all times.

- h. Writing down passwords or PINS shall be avoided as much as possible. However, written passwords or PINS shall be stored in a secure location (i.e. locked desk).
- i. Account lockout shall occur after five unsuccessful (failed password) login attempts.
- j. Password procedures and policies shall be communicated to all users who have access to restricted confidential information.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

- MEIS-002                      Access Management Policy
- MEIS-002.002              Authentication Administration Standard
- MEIS-002.003              Third Party Access Standard



**1. PURPOSE**

The purpose of this standard is to ensure appropriate implementation of authentication administration mechanisms for access to MICROS Systems, Inc systems and information assets.

**2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

**3. DEFINITIONS**

**Authentication** – The process of determining the digital identity of the sender of a communication such as a request to log in. The sender being authenticated may be a person using a computer, a computer, or a computer program.

**Authentication Factor** – A piece of information used to verify a person’s identity for security purposes.

**Biometrics** – A means of measuring unique characteristics of an individual such as a fingerprint, voiceprint, palm print, retina pattern, written signature, or other physical measures.

**4. STATEMENT OF STANDARD**

- a. A unique identifier shall be assigned to each entity accessing the MICROS Systems, Inc. enterprise to promote prevention of unauthorized access to resources and systems, and to establish accountability for activities.
  - i. A formal account creation and registration process shall be established that ensures that each User ID generated is unique.
  - ii. The process shall ensure that a manager or system owner(s) approves the creation of each account by maintaining documentation of account creations and terminations.

- iii. User ID's shall not give any indication of the users privilege level (i.e., Administrator).
- iv. System access shall be provided in accordance with a user's job description/function on a need-to-know basis.
- v. Access control rules and rights for each user or group of users shall be defined and documented.
- vi. Authorized account users shall not share their unique User ID's or passwords with any other people.
- vii. User access rights shall be reviewed on an annual basis.
- viii. Accounts that are inactive beyond ninety days shall be disabled.
- ix. A formal account de-registration process shall be established to remove terminated accounts from MICROS Systems, Inc. systems.
- x. Access rights for workers who have changed jobs or terminated employment shall be suspended or removed from the system immediately upon such change or termination. For workers who have changed jobs, their access rights shall be reviewed and modified based on their new job description and need-to-know, before being re-instated.
- xi. Active employees shall not use the User ID of a former employee.
- b. Entities are required to combine a User ID with an authentication factor to complete the authentication process.
  - i. A formal procedure to securely generate an initial authentication factor such as a password shall be utilized.
  - ii. The initial authentication factor shall be valid only for the user's initial login to the system or application.
  - iii. The initial authentication factor shall be disabled if not used within ninety days.
  - iv. The system or application shall force the user to change the authentication factor before completion of the initial login sequence.
  - v. Formal processes and procedures to administer the resetting of forgotten or locked out passwords shall be established. These processes and procedures shall ensure the positive identification or authentication of anyone requesting a reset.
  - vi. Biometrics shall be used for authentication purposes to secure a high-risk entity or environment, such as a data center facility. Biometric devices shall be combined with other authentication factors (i.e., PIN, cardkey) to create a strong two or three factor authentication mechanism.
  - vii. All non-console administrative access sessions shall be encrypted using technologies such as SSH, VPN, or SASL/TLS (transport layer security) for web based management and other non-console administrative access.
  - viii. Group, shared or generic accounts shall not be used on applications or servers containing restricted confidential data (i.e., financial, PII, payment card).

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

- MEIS-002            Access Management Policy
- MEIS-002.001    Authentication and Password Standard
- MEIS-002-003    Third Party Access Standard



## Third Party Access Standard

MEIS-002.003

---

### 1. PURPOSE

The purpose of this standard is to establish the rules for vendor and other third party access to MICROS Systems, Inc. information resources and support services, vendor responsibilities, and protection of MICROS Systems, Inc. information.

### 2. SCOPE

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 3. DEFINITIONS

**Vendor** – Any non-employee of MICROS Systems, Inc. who is providing some form of service to MICROS Systems, Inc.

**Information Resources (IR)** – Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing web sites, or otherwise capable of receiving, storing, managing or transmitting electronic data including but not limited to; mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunications resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to create, collect, record, process store, retrieve, display, and transmit information.

### 4. STATEMENT OF STANDARD

- a. Vendors shall comply with all applicable MICROS Systems, Inc. security policies, practice, standards and agreements.
- b. Vendor agreements and contracts shall specify:
  - i. How MICROS Systems, Inc. information is to be protected by the vendor.

- ii. The right for MICROS Systems, Inc. or its designated independent third party to audit vendor, which may include the right to conduct pre-assessment of vendor's security processes and procedures depending on the nature of the product or services to be provided.
- iii. Acceptable methods for the return, destruction or other disposal of MICROS Systems, Inc. information in the vendor's possession at the end of the contract.
- iv. Any information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
- c. MICROS Systems, Inc will appoint a primary point-of-contact for the vendor.
- d. Each vendor must provide MICROS Systems, Inc. with a list of all employees or contractors working on the contract. The list must be updated and provided to MICROS Systems, Inc. within forty-eight business hours of any changes.
- e. Each on-site vendor employee or contractor shall obtain a MICROS Systems, Inc. identification badge immediately upon arrival and such badge will be displayed at all times while on the premises. The identification badge shall be returned to MICROS Systems, Inc. when leaving the premises.
- f. Each on-site vendor employee or contractor shall sign in and out with the respective reception or security desk upon entering or exiting a MICROS Systems, Inc. facility.
- g. Each on-site vendor employee or contractor shall comply with all security procedures for any facility in which the vendor employee or contractor enters to perform work on behalf of MICROS Systems, Inc.
- h. Each vendor employee or contractor with access to any MICROS Systems, Inc. Restricted Confidential information shall be pre-authorized to handle that information.
- i. Vendor personnel must report all security incidents directly to the appropriate MICROS Systems, Inc. on site point of contact.
- j. Vendors supporting any production systems shall comply with all applicable MICROS Systems, Inc. change control policies and procedures.
- k. All vendor maintenance equipment on the MICROS Systems, Inc. network that connects to the outside world via the network, telephone line, or leased line and all MICROS Systems, Inc. information resource vendor accounts shall remain disabled except when in use for authorized maintenance.
- l. Vendor access shall be uniquely identifiable and password management must comply with the MICROS Systems, Inc. Authentication and Password Standard and the Authentication Administration Standard.
- m. Upon departure of a vendor employee or contractor from the contract for any reason, the vendor will ensure that all MICROS Systems, Inc. Company Confidential information in the possession of such employee or contractor is collected and returned to MICROS Systems, Inc. within two business days.
- n. Upon termination of contract or at the request of MICROS Systems, Inc., the vendor shall:
  - i. Return all MICROS Systems, Inc. information and provide written confirmation of such return within a reasonable timeframe, which shall not exceed ten business days.

- ii. Surrender all MICROS Systems, Inc. identification badges, access cards, equipment and supplies immediately.
- o. All software used by the vendor in providing services to MICROS Systems, Inc. shall be properly licensed.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

- MEIS-002                      Access Management Policy
- MEIS-002.001                Authentication and Password Standard
- MEIS-002.002                Authentication Administration Standard



**1. PURPOSE**

The purpose of this Standard is to establish requirements which shall be met by all computers connected to the MICROS Systems, Inc. networks to ensure effective malware detection and prevention. Only computer systems that meet the criteria of this standard or have been granted an exclusive waiver by M.I.S. or Information Security are approved for connectivity to MICROS Systems, Inc. networks.

**2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

**3. DEFINITIONS**

**Malware or Malicious Software** – Software designed to infiltrate or damage a computer system without the owner’s informed consent.

**Trojan** – A program that contains or installs a malicious program (sometimes called a payload or ‘trojan’). The term is derived from the classical myth of the Trojan Horse. Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

**Virus** – A computer program which reproduces. The term is commonly used to refer to a range of malware, but a true virus does not need to be harmful. To distribute itself, a virus needs to execute or otherwise be interpreted. Viruses often hide themselves inside other programs to be executed.

**4. STATEMENT OF STANDARD**

**Anti-Malware**

- a. All MICROS Systems, Inc. computers shall use an anti-malware product that is approved by the M.I.S. and Information Security departments.

- b. The anti-malware product shall be operated and configured to protect in real time on all servers and client computers.
- c. The anti-malware library definitions shall be updated at least once per day.
- d. Anti-virus scans shall be done a minimum of once per month on all user controlled workstations and servers.
- e. No one should be able to stop anti-malware definition updates and anti-malware scans except for an M.I.S. system administrator, with the approval of the Information Security department.
- f. Email servers will have additional protection against malware since email with malware shall be prevented from entering the network.

### **Email Malware Scanning**

- a. In addition to having the standard anti-virus program, the email server(s) or proxy server(s) shall also scan all external incoming and outgoing email for malware.
- b. When malware is found, the policy shall be to delete the email and not to notify either the sender or the recipient.
- c. The email server(s) or proxy server(s) will block all emails with attachment types listed in Appendix A.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

None

## 7. APPENDIX A: ATTACHMENT TYPES

<b>File Extension</b>	<b>Description</b>
.asp	Active server pages
.bas	Basic program source code is executable code
.bat	Batch file which can call executable cod
.chm	Compiled HTML help file can contain executable code
.cmd	Windows NT command script file is executable code
.com	Command file program is executable code
.cpl	Control panel extension
.dll	Dynamic link library is executable code
.exe	Binary executable program is executable code
.fxp	Microsoft FoxPro is executable code
.hlp	Help File
.hta	HTML program
.inf	Setup information
.ins	Internet naming service
.isp	Internet communications settings
.js	JavaScript file
.jse	JavaScript encoded file
.ksh	Unix shell file
.lnk	Link file
.mda	Microsoft Access add-in program
.mdb	Microsoft Access program
Mde	Microsoft Access MDE database
.mdt	Microsoft Access file
.mdw	Microsoft Access file
.mdz	Microsoft Access Wizard program
.msc	Microsoft common console document
.msi	Microsoft Windows installer package
.msp	Microsoft Windows installer patch
.mst	Visual test source files
.nws	Outlook express news file
.ops	FoxPro file
.pcd	Photo CD image or Microsoft Visual test compiled script
.pif	Shortcut to MS-DOS program
.pl	Perl scripts
.prf	Microsoft Outlook profile settings
.prg	FoxPro program source file
.reg	Registry files
Scf	Windows explorer command file
Scr	Screen saver
.sh	Shell script

Shb	Document shortcut
.sct	Windows script component
.shs	Shell scrap object
.url	Internet address
.vb	Visual basic file
.vbe	Visual basic encoded script file
.wsc	Windows script component
.wsf	Windows script file
.wsh	Windows script host settings file



## **System Audit Logging Standard**

**MEIS-003.002**

---

### **1. PURPOSE**

The purpose of this standard is to ensure that the host equipment that is owned and/or managed by MICROS Systems, Inc. has the appropriate logging enabled. This standard is designed to minimize the potential exposure to the company from damages which may result from unauthorized use of MICROS Systems, Inc. resources. Damages include the loss of sensitive company confidential data, intellectual property, damage to public image, damage to critical internal systems, etc..

### **2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### **3. DEFINITIONS**

**Host** – Any computer owned or managed by MICROS Systems, Inc.

### **4. STATEMENT OF STANDARD**

An appropriate level of logging shall be implemented and maintained on MICROS Systems, Inc. systems to provide information for upgrades and resolution of security and performance matters.

#### **4.1 Event Logging**

- a. Computer systems handling sensitive, valuable, or critical information shall securely log all significant security related events.
- b. Logs of computer security relevant events shall provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, security measures.

- c. Application and/or database management system (DBMS) software shall keep logs of user activities and statistics related to those activities which will allow the identification of suspicious activities.
- d. All production computer systems, running behind a firewall on a MICROS Systems, Inc. network and storing sensitive confidential information shall capture the following event types:
  - i. All individual user access to restricted confidential data
  - ii. All actions taken by any individual with root or administrative privileges
  - iii. User accounts accessing audit trails
  - iv. Invalid logical access attempts
  - v. Use of identification and authentication mechanisms
  - vi. Initialization of an audit log
  - vii. Creation and deletion of system-level objects
- e. All computer systems running MICROS Systems, Inc. production application systems shall include logs that record user session activity including user ID's.
- f. All system clocks shall be synchronized across the company's various processing platforms and network devices.
- g. All computer systems running MICROS Systems, Inc. production application systems shall include logs that contain the date and time, as well as user identification, event type, event success or failure, event origination and the affected data, system component or system resource.
- h. All user initiated login attempts to connect to MICROS Systems, Inc. production information systems shall be logged.
- i. A formal log rotation and archival process shall be employed for all network periphery security systems (such as firewalls) and all multi-user production servers.
- j. If they are resident on Internet-accessible computers, system logs and application logs shall be moved periodically to other machines which are not directly Internet-accessible on a schedule defined by the M.I.S. department.
- k. All audit log history shall be maintained for at least one year, with a minimum of three months of online availability.
- l. All intrusion detection, authentication, authorization, and accounting protocol server system logs shall be reviewed at least daily.

## **4.2 Monitoring**

- a. All privileged commands issued by computer system operators shall be traceable to specific individuals via the use of comprehensive logs.
- b. All changes to security settings or parameters shall be logged.
- c. Whenever system controls have been over-ridden, a log shall be generated showing the changes made.
- d. All user ID creation, deletion, and privilege change activity performed by system administrators and others with privileged user ID's shall be reflected in periodic management reports.

- e. Whenever system controls have been over-ridden, a log shall be generated showing the privileged commands that were used.
- f. All user ID creation, deletion and privilege change activity performed by system administrators and others with privileged user ID's shall be securely logged.
- g. All computer system log errors shall be reported to the applicable operational staff and the Vice President of M.I.S. in a timely fashion.
- h. M.I.S. and/or Information Security staff shall review records reflecting security relevant events on multi-user machines in a periodic and timely manner.
- i. System logs shall be configured with control mechanisms that are resistant to attacks, including attempts to de-activate, modify, or delete the logging software and/or the logs themselves.
- j. Computerized logs containing security relevant events shall be secured such that they can be read only by authorized persons.
- k. Computerized logs containing security relevant events shall be secured such that they cannot be modified.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

None



**1. PURPOSE**

The purpose of this standard is to establish a base configuration in internal host equipment that is owned and/or managed by MICROS Systems, Inc. This standard is designed to minimize the potential exposure to MICROS Systems, Inc. from damages which may result from unauthorized use of company resources. Damages may include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, etc..

**2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

**3. DEFINITIONS**

**Partner** – Any non-employee of MICROS Systems, Inc. who is providing some form of service to MICROS Systems, Inc.

**Host** – Any computer owned or managed by MICROS Systems, Inc.

**Server** – Any hardware owned or managed by MICROS Systems, Inc. that is running a server Operating System.

**4. STATEMENT OF STANDARD**

**4.1 Ownership and Responsibilities**

All internal hosts deployed on MICROS Systems, Inc. networks shall be controlled and managed by MICROS Systems, Inc. resources. Approved host configuration procedures shall be established and maintained by the M.I.S. department, and approved by the Chief Security Officer or its designate.

- a. Hosts shall be registered. The following information shall be available to positively identify one or more points of contact:
  - i. Host contact(s), backup contact and location

- ii. Hardware make, model serial number and Operating system and version in use.
  - iii. Special functions and applications, if applicable.
- b. Contact information shall be kept up to date
- c. Configuration changes for production hosts shall follow the appropriate change management procedures.

## **4.2 General Configuration Guidelines**

- a. Operating system configuration shall be in accordance with pre-defined procedures.
- b. Services and applications that will not be used shall be disabled where practical.
- c. Access to services shall be logged and/or protected through access control methods.
- d. The most recent security patches shall be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- e. Standard security principles of least required access to perform a function shall be used. Do not use a privileged account when a non-privileged account will suffice.
- f. Idle console logins shall invoke a password protected screen saver or logout the console user after fifteen minutes of inactivity.
- g. Local logins for hosts shall not be permitted. Other than built-in and maintenance accounts, users logging into hosts shall be authenticated by a Global Catalog (GC) server.
- h. Production Servers shall be in a room with restricted access (i.e. combination lock, swipe card, or key lock).
- i. Production Servers shall be powered from uninterruptible power supplies.
- j. Hosts running Microsoft Windows shall have an anti-malware software product loaded and running at all times. At no time may a client on a production network have its anti-virus scanning software disabled.
- k. Removable media shall always be virus scanned when the media is read.
- l. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access shall be performed over secure channels, (i.e., encrypted network connections using SSH or IPSec).
- m. Host operating systems shall never be configured on a network or a network accessible from insecure networks. Reasonable care shall be exercised to protect an operating system distribution from being compromised prior to complete configuration and deployment.
- n. Host operating systems shall only be loaded from a secure copy of the operating system. A secured copy of an operating system is one that, due to physical limitations, cannot be altered once written onto the media (i.e., CD-ROM) or because the source has a continuous chain of possession in secured environments with no unauthorized persons able to access the media or the device.
- o. All servers shall be hardened prior to being deployed in the staging and production environment.

### **4.3 Monitoring**

- a. All security-related events on critical or sensitive servers shall be logged and audit trails saved per the company data management and System Audit Logging Standard.
- b. Security-related events shall be reported to the M.I.S. and Information Security departments, who will review logs and report incidents to management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - i. Port-scan attacks
  - ii. Evidence of unauthorized access to privileged accounts
  - iii. Evidence of unauthorized access to user accounts from the host/client.
  - iv. Anomalous occurrences that are not related to specific applications on the host.
- c. File integrity monitoring software shall be implemented to alert personnel to unauthorized modification of critical system or content files. This software shall be configured to perform critical file comparisons at least weekly.

### **4.4 Compliance**

- a. Audits shall be performed on at least an annual basis by authorized personnel within the M.I.S. or Information Security departments, or their designated 3<sup>rd</sup> party representative.
- b. Every effort shall be made to prevent audits from causing operational failures or disruptions.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

- MEIS-006.002                      Encryption Standard



## Laptop Security Standard

MEIS-003.004

---

### 1. PURPOSE

The purpose is to establish the standard for the use of laptop computing devices and their connection to the MICROS Systems, Inc. network. These rules are necessary to preserve the integrity, availability, and confidentiality of company owned or managed information.

### 2. SCOPE

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 3. DEFINITIONS

**Partner** – Any non-employee of MICROS Systems, Inc. who is providing some type of service to MICROS Systems, Inc.

**Full Disk Encryption (or whole disk encryption)** – The encryption of all data on a hard drive.

### 4. STATEMENT OF STANDARD

- a. Laptop users shall be responsible for the physical security and condition of their laptop and the information it contains.
- b. Laptops issued to employees or partners shall remain the property of MICROS Systems, Inc. When the laptop is allocated to the individual, the user assumes temporary “custodianship” of the laptop.
- c. Laptops shall comply with the MICROS Systems, Inc. Desktop Standard.
- d. Idle console logins shall invoke a password protected screen saver or logout the console user after fifteen minutes of inactivity.
- e. To facilitate the physical security of a laptop, there shall only be one employee or partner assigned to a laptop.
- f. Users of laptops shall take the following physical security preventative measures:
  - i. Laptop computers shall not be left in view in an unattended vehicle
  - ii. Laptop computers shall not be left in an unattended vehicle (in or out of view) overnight

- iii. A laptop displaying sensitive information should be positioned, whenever possible, so that the screen cannot be viewed by others.
- iv. When leaving a laptop unattended for more than eight hours, users shall physically secure it with a cable lock and/or lock it away in a cabinet or in a locked office.
- v. In vulnerable situations, i.e., public areas such as airport lounges, hotels and conference centers, the laptop shall never be left unattended.
- vi. Portable computers shall, whenever permitted, be carried as hand luggage when traveling.
- g. If a laptop is lost or stolen, the user shall immediately notify the police, his/her immediate supervisor, and the M.I.S. Help desk as soon as possible.
- h. MICROS Systems, Inc. locations at which permanent data networks are installed shall not allow the presence of devices forming a connection between the network and any wireless network through a laptop, as this would create a bridge between two separate networks.
- i. Personal firewall software shall be installed on any company owned or managed mobile computers with Internet connectivity which are used to access the company's network(s).
- j. All laptop hard drives containing cardholder data shall use full disk encryption in accordance with the Encryption Standard.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

- MEIS-006.002      Encryption Standard
- MEIS-003.003      Desktop Security Standard



### 1. PURPOSE

The purpose of this standard is to ensure that all computer systems that connect to the MICROS Systems, Inc. network(s), regardless of operating system, including routers and switches, are protected both from malicious code and hacking attacks which exploit software vulnerabilities, through the timely installation and deployment of operating system and application security patches. Critical security patches shall be installed on computers when they become available, in accordance with this standard. These standards are designed to minimize the potential expose to MICROS Systems, Inc. from damages which may result from unauthorized use of company resources. Potential damages include, but are not limited to; the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems.

### 2. SCOPE

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 3. DEFINITIONS

**Host** – Any computer owned or managed by MICROS Systems, Inc.

**Malware (malicious software)** – Software designed specifically to damage or disrupt a computer system, such as a virus or a Trojan horse.

### 4. STATEMENT OF STANDARD

- a. Primary responsibility for patch identification and application shall be assigned to system owners and/or their designated administrators.
- b. All relevant operating system and application security patches shall be installed within one month of release where applicable.
- c. Formal change control processes shall be adhered to at all times.
- d. Security patches and software upgrades shall be thoroughly tested before applying them in the production environment.

- e. System documentation shall be updated in a timely manner to reflect applied changes.
- f. System backup images shall be made before and after the application of system upgrades and/or security patches.
- g. All system components and software shall be validated that they have the latest vendor-approved security patches.
- h. A periodic review of the patch levels of all company owned or managed assets shall be done in accordance with documented patch management procedures.
- i. Testing of all security patches and system and software configuration changes shall be done before patch deployment.

**Note:** If there is an active malware exploit with an available security patch, testing may be foregone and the M.I.S. or Information Security department may require immediate deployment of the patch.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

- System Security Policy



## System Hardening Standard

MEIS-003.006

---

### 1. PURPOSE

The purpose of this standard is to establish a base configuration for hardening servers that are in the staging or production environments. These standards are designed to minimize the potential exposure to MICROS Systems, Inc. from damages which may result from the unauthorized use of company resources. Damages include the loss of sensitive company or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc..

### 2. SCOPE

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 3. DEFINITIONS

**Partner** – Any non-employee of MICROS Systems, Inc. who is providing some form of service to MICROS Systems, Inc.

### 4. STATEMENT OF STANDARD

The system hardening standard provides the information required to harden a computer system or network device, such as a router, switch or firewall. The minimum steps include, but are not limited to:

- a. Disabling unnecessary TCP/UDP services (ports).
- b. Removing unnecessary services and daemons.
- c. Removing or unbinding unnecessary network protocols from network interface cards.
- d. Removing unnecessary network file shares.
- e. Removing unnecessary system utilities, configuration tools and diagnostic programs.
- f. Complete scanning for security weaknesses using an appropriate scanning tool, (i.e., Nessus), prior to placing the server into production.

- g. Removing unnecessary files and executables (i.e., vendor provided development tools).
- h. Removing or renaming of all unnecessary or inactive user accounts.
- i. Implementing account policies to deter password guessing and unauthorized users.
- j. Limiting the number of privileged accounts.
- k. Implementing “read-only” permissions for non-administrators or other M.I.S. staff that require access to the operating system.
- l. Changing vendor supplied defaults before installing a system on the company network(s). For example, include passwords, simple network management protocol, (SNMP), or community strings.
  - i. Wireless vendor defaults shall be changed, including but not limited to; wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Also, disable SSID broadcasts and enable Wi-Fi protected access (WPA and WPA2) technology for encryption and authentication when the device is WPA capable.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

-MEIS-003	Systems Security Policy
-MEIS-003.002	System Audit Logging Standard
-MEIS-003.003	Host Security Standard



### 1. PURPOSE

The purpose of this standard is to define the configuration to be met by all servers owned or managed by MICROS Systems, Inc. located outside of the corporate Internet firewalls. These standards are designed to minimize the potential exposure to MICROS Systems, Inc. from damages which may result from the unauthorized use of company resources. Damages include the loss of sensitive company or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc..

Internet facing devices located outside of the MICROS Systems, Inc. firewalls are considered part of the “de-militarized zone”, (DMZ), and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet, since they reside outside of the company firewalls.

### 2. SCOPE

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 3. DEFINITIONS

**De-militarized zone (DMZ)** – Any un-trusted network, connected to, but separated from, the MICROS Systems, Inc. corporate network(s) by a firewall, used for external (Internet/partner, etc.) access from within MICROS Systems, Inc., or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.

**Secure Channel** – Out-of-band console management or channels using strong encryption according to the Encryption Standard. Non-encrypted channels shall use strong user authentication (one-time passwords).

**Un-trusted network** – Any network fire-walled off from the corporate network to avoid impairment of production resources from irregular network traffic, (i.e., lab networks), unauthorized access (partner networks, the Internet, etc.), or anything else identified as a potential threat to those resources.

## **4. STATEMENT OF STANDARD**

### **4.1 General Configuration**

All servers in the DMZ shall comply with the following configuration standards:

- a. Hardware, operating systems, services and applications shall be approved by the M.I.S. and Information Security departments as part of the pre-deployment review phase.
- b. Operating system configuration shall be performed according to the Host Security and System Hardening standards.
- c. Trust relationships between systems may be introduced only according to business arrangements. All such relationships must be approved by the M.I.S. and Information Security departments.
- d. Services and applications not for general access shall be restricted by access control lists.
- e. Remote administration shall be performed over secure channels (i.e., encrypted network connections using SSH or IPSEC), or console access independent from the DMZ networks.
- f. All host content updates shall occur over secure channel.
- g. Firewalls shall be used to restrict traffic between the public network and the DMZ server, and between the DMZ server and the internal network.
- h. Security-related events shall be logged and audit trails sent to a central logging server, (i.e.; syslog). Security related events include, but are not limited to the following:
  - i. User login failures.
  - ii. Failure to obtain privileged access.
  - iii. Access policy violations.
- i. Any database containing restricted confidential data, including PII or credit card data, shall not be placed in the DMZ, but rather in the internal network behind a second firewall.

### **4.2 Equipment Outsourced to External Service Providers**

- a. The responsibility for the security of the equipment deployed by external service providers shall be clarified in the contract with the service provider as follows:
  - i. Security contacts and escalation procedures shall be documented.
  - ii. Each entity must only have access to its own restricted confidential data environment.
  - iii. Each entity's access and privileges must be restricted only to their own confidential data environment.

- iv. Logging and audit trails must be enabled and unique to each entity's restricted confidential data environment, and consistent with the terms of the Payment Card Industry Data Security Standard (PCI DSS) Requirement 10.
- v. Processes to facilitate timely forensic investigation must be established in the event of an infrastructure compromise.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

- MEIS-003 System Security Policy
- MEIS-003.002 System Audit Logging Standard
- MEIS-003.003 Host Security Standard



**1. PURPOSE**

The purpose of this standard is to define and describe network security standards that prevent clients from accessing or using services outside of those they are authorized to access or use by implementing controls such as firewalls or segmentation at strategic points of the network.

**2. SCOPE**

This standard applies to all devices or systems attached to the MICROS Systems, Inc. network(s).

**3. DEFINITIONS**

**Least privilege** – A user shall be able to see only such information and resources that are immediately necessary to perform his/her job.

**Third-party assessments** – An analysis performed by a neutral party, typically a subject-matter expert, to indicate risk and vulnerabilities in a system.

**Simple Network Management Protocol (SNMP)** – Layer seven, or the application layer, of the IP stack.

**Network Segmentation** – Techniques of splitting a computer network into sub-networks, each being a network segment or network layer.

**Access Control list (ACL)** – A concept in computer security used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request.

#### **4. STATEMENT OF STANDARD**

- a. All systems and devices shall have implemented access control. Access shall be provided at the least amount of privilege needed by the individual.
- b. Logging shall be implemented on all systems that have such capability. Login accounting and network statistics shall be logged, at a minimum.
- c. Local and remote authentication shall be handled in accordance with the Access Management Policy, (MEIS-002).
- d. All Gateway systems shall be hardened in accordance with the System Security Policy and Standards, (MEIS-003).
- e. Only connections and protocols that have been approved by the M.I.S. and Information Security departments are allowed on the company network(s).
- f. Networks shall be segregated according to industry and regulatory standards.
- g. New network architectures shall be reviewed and approved by the M.I.S. and Information Security departments before implementation.
- h. Security assessments shall be performed on a periodic basis and security vulnerabilities repaired in order to continually promote optimal system security.
- i. Access control mechanisms, such as ACL, routing controls, filtering mechanisms, or gateways, shall be implemented in cases where organizations share a common network infrastructure.

#### **5. REFERENCE**

- |               |  |
|---------------|--|
| -MEIS-004     | Network Security Policy                  |
| -MEIS-008.001 | Information Security Assessment Standard |



**1. PURPOSE**

This standard prohibits access to MICROS Systems, Inc. network(s) via unsecured wireless communications mechanisms. Only wireless systems that met the criteria of this standard or have been granted a written waiver by both the M.I.S. and Information Security departments are approved to connect to company network(s).

**2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

**3. DEFINITIONS**

**Media Access Control (MAC) address** – A hardware address that uniquely identifies each node of a network.

**Virtual private Network (VPN)** – A method of building a private network on top of a public network such that the private network is separated and protected.

**EAP** – A universal authentication framework used in wireless networks and point-to-point connections defined by RFC 3748.

**4. STATEMENT OF STANDARD**

**4.1 Approved Technology**

- a. All wireless network access shall only occur through the use of vendor products and configurations approved by the M.I.S. and Information Security departments.
- b. All wireless data communication devices, (i.e., personal computers, cellular phones, PDA's, etc.) connected to the MICROS Systems, Inc. network(s) shall comply with all applicable company information policies, procedures and standards.

- c. All wireless access-points and base stations connected to the MICROS Systems, Inc. network(s) shall be registered and approved by the M.I.S. and Information Security departments.

#### **4.2 Monitoring of Uncontrolled Wireless Devices**

- a. Unauthorized wireless devices shall not be allowed on the MICROS Systems, Inc. network(s).

#### **4.3 Authentication of Wireless Clients**

- a. The strongest form of wireless authentication permitted by the client device shall be used.
- b. EAP methods that exchange authentication credentials outside of encrypted tunnels may not be used.

#### **4.4 Encryption**

- a. All wireless communication between MICROS Systems, Inc. devices and network(s) shall be encrypted.
- b. The strongest form of wireless encryption permitted by the client device shall be used.

#### **4.5 Access Control Policies**

- a. Access to MICROS Systems, Inc. network resources through wireless networks shall be restricted based on the business role of the user.
- b. Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block.
- c. The access control system shall be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
- d. Wireless networks must be segmented from restricted confidential data by installing perimeter firewalls and configuring those firewalls to deny any traffic from the wireless network.

#### **4.6 Guest Access**

- a. All wireless guest access shall be authenticated.
- b. Guest access shall be restricted to approved network protocols.

#### **4.7 Encryption and Authentication**

- a. All computers with wireless LAN devices shall utilize a company approved VPN.
- b. Wireless implementations shall maintain at least 128-bit point-to-point hardware encryption.

- c. All implementations shall support a hardware address that can be registered and tracked, (i.e., a MAC address).
- d. All implementations shall support and employ strong user authentication.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

-MEIS-003.001	Malware Protection Standard
-MEIS-004	Network Security Policy



**1. PURPOSE**

This section defines and describes the standards to be implemented to support the firewall policy of MICROS Systems, Inc.

**2. SCOPE**

This standard applies to all firewalls connected to the MICROS Systems, Inc. network(s).

**3. DEFINITIONS**

**De-militarized Zone (DMZ)** - Any un-trusted network, connected to, but separated from, the MICROS Systems, Inc. corporate network(s) by a firewall, used for external (Internet/partner, etc.) access from within MICROS Systems, Inc., or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.

**Firewall** – A logical barrier designed to prevent unauthorized or unwanted communications between sections of a computer network.

**4. STATEMENT OF STANDARD**

- a. All network traffic shall be denied by default, and rules defined according to business and security requirements.
- b. All unused ports and services shall be blocked (or dropped).
- c. Administrative access shall be strictly controlled and allowed only to authorized personnel.
- d. A firewall must be positioned between all trusted and un-trusted networks.
- e. Change control shall be adhered to for all rule changes, updates to firewall, operating system and code, and for any patches or fixes applied.
- f. Logging shall be enabled and routinely reviewed for unauthorized activities.
- g. Periodic audits of the firewall configuration shall be performed.
- h. Stateful Inspection, also known as Dynamic Packet Filtering, will be used, thereby allowing only “established” connections into the MICROS Systems, Inc. network(s).
- i. Firewalls that support anti-spoofing (anti-masquerading) measures shall be used.
- j. All router configuration files shall be secured and synchronized for normal functionality as well as re-starts.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

-MEIS-004                      Network Security Policy



**1. PURPOSE**

The purpose of this standard is to define accepted practices for connecting to MICROS Systems, Inc. network(s) from any host. These standards are designed to minimize the potential exposure to the company from damages which may result from the unauthorized use of company resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal company systems, etc..

**2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

Remote access implementations covered by this policy include but are not limited to; dial-in modems, frame-relay, DSL, VPN, SSH, and cable modems, etc..

**3. DEFINITIONS**

**DSL (Digital Subscriber Line)** – A technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office. DSL speeds are based on the distance between the customer and telephone company central office.

**SSH (Secure Shell)** – Secure Shell provides secure remote logins for general and administrative use, as well as secure remote execution and copying. Many people use Secure Shell to replace Telnet, FTP, and the Berkeley Services “r” commands. The “r” commands are rlogin (remote login), rsh (remote shell), rcp (remote copy), and rexec (remote execution).

**VPN (Virtual Private Network)** – A method of building a private network on top of a public network such that the private network is protected and secure.

**Split-tunneling** – The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN.

**Dual homing** – The connection of a terminal so that it is served by either of two switching centers.

#### **4. STATEMENT OF STANDARD**

- a. Remote access shall be strictly controlled through two-factor user authentication.
- b. VPN access shall employ minimum encryption strength of 128-bit.
- c. Split-tunneling or dual-homing is not permitted at any time.
- d. Non-standard hardware configurations shall be approved by the M.I.S. and Information security departments.
- e. All equipment used to connect remotely to the MICROS Systems, Inc. network(s) shall meet the minimum host requirements as specified in MEIS-003.003, “Host Security Standard”.
- f. Remote maintenance accounts used by vendors shall be enabled for remote maintenance only during the time periods when needed.
- g. Remote connectivity to restricted confidential information through modems and wireless connectivity shall employ an approved process with the following checkpoints:
  - i. Management level approval has been obtained for the technology’s use;
  - ii. All devices have been documented with their owner, contact information, and purpose as well as the personnel with access thru them;
  - iii. Acceptable uses and locations of the technologies have been determined;
  - iv. Modem sessions shall be automatically disconnected after a specified period of inactivity;
  - v. Modems used by vendors shall only be activated when needed and immediately deactivated after each use.
  - vi. Cardholder data storage shall be prohibited on local hard drives, floppy disks, or other external media or remote devices.

#### **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

#### **6. REFERENCE**

- MEIS-002.002 Authentication and Password Standard
- MEIS-002.003 Third Party Access Standard
- MEIS-003 Systems Security Policy

-MEIS-003.003  
-MEIS-004

Host Security Standard  
Network Security Policy



**1. PURPOSE**

This section defines and describes the standards to support access to MICROS Systems, Inc. applications.

**2. SCOPE**

This standard applies to the method that applications should be accessed and how application data should be stored as part of the MICROS Systems, Inc. enterprise network(s).

**3. DEFINITIONS**

**Digital signature** – An electronic signature that can be used to authenticate the identity of the sender of a message or the signatory of a document, or ensure that the original content of the message or document is unchanged.

**PAN** – An acronym which stands for Primary Account Number. It is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also referred to as account number.

**PIN** – An acronym which stands for Personal Identification Number. It is used for authentication on such devices as an ATM (Automated Teller Machine).

**4. STATEMENT OF STANDARD**

- a. Application authentication shall adhere to the terms of MEIS-002.001, Authentication and Password Standard.
- b. Applications shall execute with the lowest access privilege possible to sufficiently perform its tasks.
- c. Application database access shall only be granted with proper account authorization and access management.
- d. Users requiring elevated privileges in an application shall be granted these privileges based on their roles and responsibilities on a need-to-know basis.
- e. Physical access to application servers shall be controlled.
- f. Change control processes shall be followed for application changes.

- g. File and folder permissions shall be set to the minimum level required for proper application access.
- h. Group permissions shall not be granted through default vendor groups such as Windows Everyone, Users, and Domain Users Groups.
- i. Non-publicly routable IP addresses shall be used for communication between applications and their databases.
- j. Access to back-end application utilities and source code shall be restricted to only those entities that require such access for their job functions.
- k. Source code and program libraries shall never be stored on the production servers, but rather in the appropriate source code management repository.
- l. Sensitive credit card authentication data, including the full contents of any track from the magnetic stripe, card validation code or value, PIN, or encrypted PIN block shall not be stored by an application subsequent to authorization.
- m. PAN data shall be masked when being displayed in an application. The first six and the last four PAN digits are the maximum number of digits allowed for display.
- n. PAN data shall be rendered unreadable anywhere it is stored (including portable media, backup media, in logs, and data traveling across wireless networks). One of the following methods shall be used to obfuscate this data:
  - i. Strong one-way hash functions (hashed indexes)
  - ii. Truncation
  - iii. Index tokens and pads (pads must be securely stored)
  - iv. Strong cryptography with associated key management processes and procedures.

## 5. INTERPRETATION

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## 6. REFERENCE

-MEIS-002.001	Authentication and Password Standard
-MEIS-005	Application Security Policy
-MEIS-005.002	Database Security Control Standard



**1. PURPOSE**

This section defines and describes the standards to be implemented to support database security controls of enterprise applications used by MICROS Systems, Inc.

**2. SCOPE**

This standard applies to how databases should be accessed as part of the MICROS Systems, Inc. network(s).

**3. DEFINITIONS**

**Audit Trail** – A record of transactions in an information system that provides verification of the activity of the system.

**Personally Identifiable Information (PII)** – Any information that, in itself or as part of a unique combination of information, specifically recognizes an individual by unique descriptors and/or identifiers.

**Third party** – Any non employee of MICROS Systems, Inc. who is providing some form of service to the company.

**Principle of “Least Privilege”** – A concept whereby users are assigned the lowest level of privileges commensurate with their assigned duties and functions.

**4. STATEMENT OF STANDARD**

- a. Database activity shall be monitored, at a level commensurate with the classification of the data, through audit logging and periodic reviews.
- b. Database controls shall ensure that only authorized users are permitted to enter or view information on the database. These controls may be defined down to the record level and/or data field level as necessary.
- c. Restricted confidential data shall not be used for testing purposes.
- d. The necessary security precautions shall be in place for any automatic production to test synchronization routines.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

-MEIS-005            Application Security Policy  
-MEIS-005.001      Application Access Standard



## Data Backup and Recovery Standard

MEIS-006.001

---

### 1. PURPOSE

The purpose of this section is to establish a security standard for data backups and recovery for MICROS Systems, Inc. information resources.

### 2. SCOPE

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 3. DEFINITIONS

**Retention Period** – The amount of time a document or data should be kept, and then archived or destroyed.

### 4. STATEMENT OF STANDARD

- a. Data backups shall be accompanied by a complete and accurate record of the contents to be stored along with backup media.
- b. All backup media shall be labeled and properly secured based on the highest sensitivity classification of the data stored on the media.
- c. Backup media shall be tested, by exercising the restoration process at least semi-annually, to validate the reliability of the procedure and backup media.
- d. Offsite storage vendors shall be bonded and sign an agreement that is acceptable with the MICROS Systems, Inc. Legal department.

### 5. INTERPRETATION

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

### 6. REFERENCE

- MEIS-006 Data Security Management Policy
- MEIS-006.002 Encryption Standard



## Encryption Standard

MEIS-006.002

---

### 1. PURPOSE

The purpose of this standard is to establish regulations for encrypting data files for MICROS Systems, Inc. information resources.

### 2. SCOPE

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

### 3. DEFINITIONS

**The internal network** – The trusted networks owned or managed by MICROS Systems, Inc.

### 4. STATEMENT OF STANDARD

- a. Data classified as Restricted Confidential Information stored or transmitted outside of the internal network shall be encrypted.
- b. Systems that incorporate file encryption technologies shall meet the following minimum algorithms:
  - i. AES (Rinjndael)
  - ii. 3DES
  - iii. Hash values of SHA 1
- c. Disk encryption shall be used when large amounts of sensitive cardholder data are stored on networked disks (i.e., workstations, laptops, servers).
- d. Disk encryption logical access shall be managed independently of native operating system access control mechanisms (i.e., not using local system or Active Directory accounts). In addition, encryption keys shall not be tied to user accounts.
- e. Wireless communications shall be at least 128-bit encrypted.
- f. Technologies that provide secure transmission over public or un-trusted networks shall implement encryption commensurate with the type of data being transmitted.
- g. Authentication sessions shall be encrypted.

- h. In the event that, due to extenuating business circumstances, (and provided that there are no legal requirements to the contrary), a MICROS Systems, Inc. client is unable or unwilling to implement encryption when the company policies so require, the matter shall be turned over to the MICROS Systems, Inc. Legal department for further review and action.
- i. The timeframe that a data element is valid shall be considered when determining the level of encryption to use. For example, information that is only valid for ten seconds does not require high-end encryption methods.
- j. Encryption keys shall be protected and secured against both disclosure and misuse.
- k. Encryption key access shall be restricted to the fewest number of custodians necessary.
- l. Encryption keys shall be stored securely in the fewest possible locations and forms.
- m. All implementations of encryption key management processes and procedures shall be documented.

**5. INTRPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

**6. REFERENCE**

-MEIS-006	Data Security Management Policy
-MEIS-006.001	Data Backup and Recovery Standard
-MEIS-004.002	Wireless Security Standard
-MEIS-003.004	Laptop Security Standard
-	PCI Data Security Standard



**1. PURPOSE**

The purpose of this section is to establish standards for timely and appropriate company response to any security-related incidents that may occur.

**2. SCOPE**

This standard applies to anyone accessing or using MICROS Systems, Inc. information technology resources and facilities including, but not limited to, employees, contractors, consultants, temporary employees, customers, visitors, and vendor personnel. This policy applies to all equipment that is owned or leased by MICROS Systems, Inc. and to all third party equipment connected to company business systems.

**3. DEFINITIONS**

**Red Alert Incident** – A security-related incident whereby the entire MICROS Systems, Inc. information enterprise, or multiple elements or business units of the information enterprise are affected. This includes; a virus attack, an attack on the Internet infrastructure, an unwanted disruption or denial of service attack, employee or partner threats, defacement of or unauthorized use or alteration of the company web page(s), discovery of a Trojan Horse program or similar unauthorized software, unauthorized access to company enterprise systems, network devices, or data; theft, exposure or destruction of confidential or sensitive company, partner, or customer data (in company possession); use of company systems to probe or attach other computer systems or networks; violations of physical security; or other information security incidents with significant impact to the company.

**Security Incident Response Team (SIRT)** – The SIRT consists of representatives of the M.I.S., Information Security, Legal, Facilities, and HR departments, along with any contracted third parties as may be deemed necessary.

**4. STATEMENT OF STANDARD**

- a. The SIRT shall simulate a Red Alert incident at least twice per year.
- b. Appropriate training shall be provided to staff with security breach and incident response responsibilities.
- c. Alerts from network security devices shall be incorporated as evidence in the incident response process.

- d. The incident response process shall be reviewed and modified to evolve according to lessons learned and to incorporate industry changes and developments.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

-MEIS-007      Information Security Incident Handling Policy



## Information Security Assessment Standard      MEIS-008.001

---

### 1. PURPOSE

This standard describes the practices to be implemented to support the information security policies of MICROS Systems, Inc. Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes and custom software should be tested frequently to ensure security continuity is maintained over time.

### 2. SCOPE

This standard applies to the methods by which security assessments are to be performed when evaluating the MICROS Systems, Inc. corporate processes and information assets, and third parties who connect to company resources or handle restricted company confidential information.

### 3. DEFINITIONS

**Personally identifiable information (PII)** – Any information that, in itself or as part of a unique combination of information, specifically recognizes an individual by unique descriptors and/or identifiers.

**Penetration testing** – A method of evaluating the security of a computer system or network by simulating an attack by a hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.

### 4. STATEMENT OF STANDARD

MICROS Systems, Inc. shall routinely review physical security and information systems and processes for compliance with statutory and regulatory requirements, and with established security policies and standards. An evaluation shall also be performed on any third parties who handle any restricted confidential data that is either owned or under the control of MICROS Systems, Inc.

#### **4.1 Internal Review**

Self-assessments of safeguards (procedural, electronic, and physical) shall be performed and compliance with security policies and standards assessed. Owners of information systems or designates shall continuously monitor their systems and processes for compliance with applicable security policies and standards.

#### **4.2 Independent Review**

Independent third party audits shall be conducted periodically to validate security architecture, determine level of compliance and to verify that company security policies and standards, as well as any contractual obligations, statutory or regulatory requirements are being followed.

#### **4.3 Vulnerability Scanning**

Internal and external vulnerability scans shall be performed at least once per year, and after any significant change in the network (such as new production system component or server installations, changes in network topology, firewall rule modifications, product upgrades, etc.).

#### **4.4 Penetration Testing**

Penetration testing shall be performed at least once per year, and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

#### **4.5 Physical Building Vulnerability Testing**

Building security systems shall be routinely tested for security vulnerabilities. Only authorized personnel approved by the Information Security and Facilities departments may perform testing. Formal change control processes shall be followed.

#### **4.7 Wireless Testing**

An analysis of all wireless devices in use, and their security configurations, will be conducted at least once per quarter.

#### **4.8 Application Security Testing**

Security test conditions must be part of user acceptance and QA plans to test for application security vulnerabilities. These include, but are not limited to tests for:

- a. Data input validation
- b. Broken access control (i.e., malicious use of user ID's)

- c. Broken authentication and session management (use of account credential and session cookies)
- d. Cross-site scripting (XSS) attacks
- e. Buffer overflows
- f. Injection flaws (i.e., SQL injection)
- g. Improper error handling
- h. Insecure storage
- i. Denial of service
- j. Insecure configuration management

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

-MEIS-008      Security Operations Policy



**1. PURPOSE**

This standard defines and describes the practices to be implemented to support the security operations policy of MICROS Systems, Inc. The processes within this document are meant to strengthen the integrity and privacy of MICROS Systems, Inc. corporate and administrative data by providing a specific set of steps to be completed before a system is developed, acquired or implemented in a company facility, or an a company network.

**2. SCOPE**

This standard applies to systems that are deployed within any MICROS Systems, Inc. facilities or company network.

**3. DEFINITIONS**

**Exception Management** – A process required to deploy a system that does not meet MICROS Systems, Inc. information security standards and policies. The exception form, or risk letter, identifies risks and must document a valid business justification for not meeting the corporate policy and standards.

**4. STATEMENT OF STANDARD**

- a. When any new system is proposed for deployment in a MICROS Systems, Inc. owned or managed Data Center, the system owners will provide appropriate documentation (including architectural diagrams indicating such network devices as firewalls and wireless access points), and the system shall be assessed by the M.I.S. department for architectural weaknesses, vulnerabilities, and proper configuration. Any custom code shall be reviewed prior to release to production or customers in order to identify any potential coding vulnerabilities.
- b. Any exceptions to established policies and standards shall be documented prior to system deployment through the Information Security exception process. A valid business justification and approval from the VP of M.I.S. and Chief Security Officer are also required for exceptions to this policy.
- c. When any new system is proposed for deployment on MICROS Systems, Inc. network infrastructure, a system architecture review shall be performed by the M.I.S. department to determine the appropriate security controls to be applied to the system and to determine the proper location within the corporate environment.

- d. Upon deployment of a new system in a MICROS Systems, Inc. Data Center, the M.I.S. team will perform a system security audit on the device to ensure that it meets all security policies and standards.
- e. Upon deployment of a new system in a MICROS Systems, Inc. Data Center, the following shall be removed before the production systems become active:
  - i. Test data and accounts
  - ii. Custom application accounts, user names and passwords
  - iii. Any vendor default accounts, user names and passwords
- f. Third parties that manage devices located in MICROS Systems, Inc. facilities are subject to the requirements of this standard.

## **5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## **6. REFERENCE**

-MEIS-008.000                      Security Operations Policy



**PURPOSE**

This standard defines and describes the practices to be implemented to support the security operations policy of MICROS Systems, Inc. Responsibilities shall be defined and control mechanisms shall be implemented to ensure that company owned and managed computer processing and information assets are operated and administered in a secure manner in compliance with company policies and procedures.

**SCOPE**

This standard applies to how MICROS Systems, Inc. systems should be managed from an information security perspective.

**DEFINITIONS**

**Intrusion Detection System (IDS)** – A security tool designed to detect security breaches. Some IDS systems may be configured to respond and deflect attacks.

**Intrusion Prevention System (IPS)** – A security tool designed to block attacks and prevent security breaches.

**STATEMENT OF STANDARD**

- a. MICROS Systems, Inc. systems shall be operated and administered using documented procedures protecting the information assets of the company.
- b. Controls shall be in place so that no employee or group shall be in a position to both perpetrate and to conceal errors or fraud.
- c. Test systems shall be logically and virtually separated from production systems.
- d. All security operations shall be incorporated into the company testing, acceptance and change control processes.
- e. Procedures, roles and responsibilities will be defined to guide day-to-day operational security processes, including issues such as account management, authorization, remote access, systems deployment, and assessment.
- f. The management of electronic keys to control both the encryption and decryption of sensitive messages and/or files shall be performed under dual control, with the duties being rotated between staff.

- g. Network intrusion detection, intrusion prevention systems, or host-based intrusion detection systems will be used to monitor network traffic and alert personnel of suspected intrusion attempts or compromises.
- h. All intrusion detection and prevention engines shall be kept up to date.

### **INTERPRETATION**

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

### **REFERENCE**

-MEIS-008.000                      Security Operations Policy



## Personal Information Protection Standard      MEIS-009.001

---

### 1. PURPOSE

This standard is intended to facilitate the protection of “Personal Information” while in the control or possession of the company.

### 2. SCOPE

This standard defines the methods that Personal Information may be accessed, used, disclosed and disposed of while in the control or possession of the company.

### 3. DEFINITIONS

**Personal Information** – Personal Information is defined as a person’s first and last name, or first initial and last name, when found in combination with one or more of the following data elements: Social Security number, driver’s license number, state-issued identification card number, financial account number, or credit or debit card number. Excluded from this definition of Personal Information is any information made available to the general public.

### 4. STATEMENT OF STANDARD

- a. **Access to Personal Information:** Access to information or documents containing Personal Information shall be restricted to only those employees who have a legitimate business reason to access such information or documents. MICROS supervisors/administrators are responsible for implementing this restriction through appropriate training and oversight procedures.
- b. **Prohibited Disclosures:** MICROS employees shall maintain the confidentiality of information and documents containing Personal Information. MICROS employees shall not take any of the following actions with the Personal Information of an employee, or other individual:
  - i. Publically display the Personal Information.
  - ii. Use the Personal Information as an individual’s primary identification badge, membership card, permit or license.

- iii. Visibly print the Personal Information on any identification badge, membership card, permit or license.
- iv. Mail a document containing an individual's Personal Information unless it falls within one of the following exceptions:
  - a. State or federal law, rule, regulation or court order or rule authorizes, permits or requires that the Personal Information appear in the document.
  - b. The document is sent as part of an application or enrollment process initiated by the individual.
  - c. The document is sent to establish, confirm the status of, service, amend or terminate an account, contract, policy or employee or health insurance benefit or to confirm the accuracy of a social security number of an individual who has an account, contract, policy or employee or health insurance benefit.
  - d. The document is mailed in connection with an ongoing administrative use to do any of the following:
    - i. Verify an individual's identity, identify an individual or accomplish another similar administrative purpose related to an existing or proposed account, transaction, product, service or employment.
    - ii. Investigate an individual's claim, credit, criminal or driving history.
    - iii. Detect, prevent or deter identify theft or another crime.
    - iv. Lawfully pursue or enforce MICROS' legal rights.
    - v. Provide or administer employee or health insurance benefits, claims or retirement programs.
  - e. The document is mailed by or at the request of the individual whose Personal Information appears in the document or at the request of his/her parent or legal guardian.
  - f. The document is mailed in a manner or for a purpose consistent with the federal Gramm-Leach-Bliley Act (GLB), federal Health Insurance Portability and Accountability Act (HIPAA), or the state insurance code.
  - g. Other exceptions approved by the MICROS Legal Department.
- v. Transmit or require an individual to transmit his/her Personal Information over the Internet or a public computer system or network unless the connection is secure or the transmission is encrypted.

- vi. Transmit or require an individual to use or transmit his/her Personal Information to gain access to an Internet website or a public computer system or network unless the connection is secure or the transmission is encrypted.
  - vii. Store any Personal Information on laptops or portable devices that is not encrypted.
  - viii. Mail any document containing Personal Information that is visible on or from outside the envelope or packaging for the document.
- c. **Authorized Uses:** This policy does not prohibit the use of Personal Information where the use is authorized or required by state or federal statute, rule, regulation or court order or rule or pursuant to legal discovery or process. This policy also does not prohibit the use of Personal Information by the Department of Police and Public Safety from criminal investigation purposes or the provision of Personal Information to a Title IV-agency (child support/support orders), law enforcement agency, court or prosecutor as part of a criminal investigation or prosecution.
- d. **Disposal of Personal Information:** Documents that contain Personal Information shall be properly destroyed when those documents no longer need to be retained pursuant to MICROS document retention policies. Paper documents containing Personal Information should be shredded. Electronic documents containing Personal Information should be destroyed in a manner that renders them unreadable and unrecoverable, or in a manner consistent with any “best practices” guidance issued by the Chief Information Security Officer, or the Vice President, MIS.
- e. **Violations:** Violations of this Policy may result in disciplinary action, up to and including termination of employment.

## 5. INTERPRETATION

All questions pertaining to this standard should be directed to the Chief Security Officer, the VP of M.I.S. or their designates.

## 6. REFERENCE

None



## Medical Information Privacy Standard      MEIS-010.001

---

### 1. PURPOSE

This standard is intended to facilitate the protection of medical information while in the control or possession of the company.

### 2. SCOPE

This standard defines the methods that medical information may be accessed, used, disclosed and disposed of while in the control or possession of the company.

### 3. DEFINITIONS

**Protected Health Information, (PHI):** confidential health information that identifies an employee or could be used to identify an employee and relates to a physical or mental health condition or the payment of an employee's health care expenses.

### 4. STATEMENT OF STANDARD

- a. **Summary:** The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires health plans to notify plan participants and beneficiaries about its policies and practices to protect the confidentiality of their health information. This document is intended to satisfy HIPAA's notice requirement with respect to all health information created, received, or maintained by the MICROS group health plan (the "Plan"), as sponsored by MICROS Systems, Inc. (the "Company").

The Plan needs to create, receive, and maintain records that contain health information about participants in order to administer the Plan and provide participants with health care benefits. This notice describes the Plan's health information privacy policy with respect to Medical, Prescription Drug, Dental, Vision and/or Health Care Flexible Spending Arrangement (FSA) benefits. This notice advises participants the ways the Plan may use and disclose health information about them, describes their rights, and the obligations the Plan has regarding the use and disclosure of their

health information. However, it does not address the health information policies or practices of their health care providers.

b. **MICROS Pledge Regarding Health Information Privacy:** The privacy policy and practices of the Plan protect confidential health information that identifies participants or could be used to identify participants and relates to a physical or mental health condition or the payment of health care expenses. This individually identifiable health information is known as “protected health information” (PHI). Participant PHI will not be used or disclosed without a written authorization from the participant, except as described in this notice or as otherwise permitted by federal and state health information privacy laws.

c. **Privacy Obligations of the Plan:**

The Plan is required by law to:

- make sure that health information that identifies participants is kept private;
- give participants this notice of the Plan’s legal duties and privacy practices with respect to health information about them; and
- follow the terms of this notice that are currently in effect.

d. **How the plan May Use and Disclose Health Information About It’s Participants:**

The following are the different ways the Plan may use and disclose participant’s PHI:

- **For Treatment:** The Plan may disclose a participant’s PHI to a health care provider who renders treatment on the participant’s behalf. For example, if the participant is unable to provide medical history as the result of an accident, the Plan may advise an emergency room physician about the types of prescription drugs the participant currently takes.
- **For Payment:** The Plan may use and disclose a participant’s PHI so claims for health care treatment, services, and supplies the participant receives from health care providers may be paid according to the Plan’s terms. For example, the Plan may receive and maintain information about surgery a participant received to enable the Plan to process a hospital’s claim for reimbursement of surgical expenses incurred on the participant’s behalf.
- **For Health Care Operations:** The Plan may use and disclose a participant’s PHI to enable it to operate or operate more efficiently or make certain all of the Plan’s participants receive their health benefits. For example, the Plan may use a participant’s PHI for case management or to perform population-based studies designed to reduce health care costs. In addition, the Plan may use or disclose a participant’s PHI to conduct compliance reviews, audits, actuarial studies, and/or for fraud and abuse detection. The Plan may also combine health information about many Plan participants and disclose it to the Company in summary fashion

so it can decide what coverage the Plan should provide. The Plan may remove information that identifies participants from health information disclosed to the Company so it may be used without the Company learning who the participants are specifically.

- **To the Company:** The Plan may disclose a participant's PHI to designated Company personnel so they can carry out their Plan-related administrative functions, including the uses and disclosures described in this notice. Such disclosures will be made only to the Company's Plan Supervisor, B. Ray Stephens and/ or members of the Company's Benefits Department. These individuals will protect the privacy of the participant's health information and ensure it is used only as described in this notice or as permitted by law. Unless authorized by the participant in writing, the participant's health information: (1) may not be disclosed by the Plan to any other Company employee or department and (2) will not be used by the Company for any employment-related actions and decisions or in connection with any other employee benefit plan sponsored by the company.
- **To a Business Associate:** Certain services are provided to the Plan by third party administrators known as "business associates." For example, the Plan may input information about a participant's health care treatment into an electronic claim processing system maintained by the Plan's business associate so the participant's claim may be paid. In doing so, the Plan will disclose the participant's PHI to its business associate so it can perform its claim payment function. However, the Plan will require its business associates, through contract, to appropriately safeguard the participant's health information.
- **Treatment Alternatives:** The Plan may use and disclose a participant's PHI to tell the participant about possible treatment alternatives that may be of interest to them.
- **Health-Related Benefits and Services:** The Plan may use and disclose a participant's PHI to tell the participant about health-related benefits or services that may be of interest to them.
- **Individual Involved in Your Care or Payment of Your Care:** The Plan may disclose PHI to a close friend or family member involved in or who helps the participant pay for health care. The Plan may also advise a family member or close friend about a participant's condition, location (for example, that the participant is in the hospital), or death.
- **As Required by Law:** The Plan will disclose a participant's PHI when required to do so by federal, state or local law, including those that require the reporting of certain types of wounds or physical injuries.

e. **Special Use and Disclosure Situations:**

The Plan may also use or disclose a participant's PHI under the following circumstances:

- **Lawsuits and Disputes:** If a participant becomes involved in a lawsuit or other legal action, the Plan may disclose the participant's PHI in response to a court or administrative order, a subpoena, warrant, discover request, or other lawful due process.
- **Law Enforcement:** The Plan may release a participant's PHI if asked to do so by a law enforcement official, for example, to identify or locate a suspect, material witness, or missing person or to report a crime, the crime's location or victims, or the identity, description of the person who committed the crime.
- **Workers' Compensation:** The Plan may disclose a participant's PHI to the extent authorized by and to the extent necessary to comply with workers' compensation laws or other similar programs.
- **Military and Veterans:** If a participant is currently, or becomes a member of the U.S. armed forces, the Plan may release medical information about the participant as deemed necessary by military command authorities.
- **To Avert Serious Threat to Health or Safety:** The Plan may use and disclose a participant's PHI when necessary to prevent a serious threat to the participant's safety, or the health and safety of the public or another person.
- **Public Health Risks:** The Plan may disclose health information about a participant for public activities. These activities include preventing or controlling disease, injury or disability; reporting births and deaths; reporting child abuse or neglect; or reporting reactions to medication or problems with medical products or to notify people of recalls of products they have been using.
- **Health Oversight Activities:** The Plan may disclose a participant's PHI to a health oversight agency for audits, investigations, inspections, and licensure necessary for the government to monitor the health care system and government programs.
- **Research:** Under certain circumstances, the Plan may use and disclose a participant's PHI for medical research purposes.
- **National Security, Intelligence Activities, and Protective Services:** The Plan may release a participant's PHI to authorized federal officials: (1) for intelligence, counterintelligence, and other national security activities authorized by law and (2) to enable them to provide protection to the members of the U.S. government or foreign heads of state, or to conduct special investigations.

- **Organ and Tissue Donation:** If the participant is an organ donor, the Plan may release medical information to organizations that handle organ procurement or organ, eye, or tissue transplantation or to an organ donation bank to facilitate organ or tissue donation and transplantation.
- **Coroners, Medical Examiners, and Funeral Directors:** The Plan may release a participant's PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or to determine the cause of death. The Plan may also release a participant's PHI to a funeral director, as necessary, to carry out his/her duty.

**f. Participant Rights Regarding Their Health Information:**

Participant rights regarding the health information the Plan maintains about its participants is as follows:

- **Right to Inspect and Copy:** A participant has the right to inspect and copy our PHI. This includes information about the participant's plan eligibility, claim and appeal records, and billing records, but does not include psychotherapy notes.

To inspect and copy health information maintained by the Plan, the participant should submit a request in writing to the Plan administrator. The Plan may charge a fee for the cost of copying and/or mailing this information. In limited circumstances, the Plan may deny a request to inspect and copy a participant's PHI. Generally, if a participant is denied access to health information, the participant may request a review of the denial.

- **Right to Amend:** If a participant feels that health information the Plan has about them is incorrect or incomplete, they may ask the Plan to amend it. Participants have the right to request an amendment for as long as the information is kept by or for the Plan.

To request an amendment, send a detailed request in writing to the Plan Administrator. The participant must provide the reason(s) to support the request. The Plan may deny the request if the participant requests that the Plan amends health information that was: accurate and complete, not created by the Plan; not part of the health information kept by or for the Plan; or not information that the participant would be permitted to inspect and copy.

- **Right to an Accounting of Disclosures:** Participants have the right to request an "accounting of disclosures." This is a list of disclosures of their PHI that the Plan has made to others, except for those necessary to carry out health care treatment, payment or operations; disclosures made to the participant; or in certain other situations.

To request an accounting of disclosures, participants must submit their request in writing to the Plan Administrator. The request must state a time period, which may not be longer than six years prior to the date the accounting was requested.

- **Right to Request Restrictions:** Participants have the right to request a restriction on the health information the Plan uses or discloses about them for treatment, payment, or health care operations. Participants also have the right to request a limit on the health information the Plan discloses about them to someone who is involved in their care or the payment for their care, like a family member or friend. For example, a participant could ask that the Plan not use or disclose information about a surgery they have had.

To request restrictions, participants must make their request in writing to the Plan Administrator. They must advise: (1) what information they wish to limit; (2) whether they want to limit the Plan's use, disclosure, or both; and (3) to whom they want the limit(s) to apply.

**Note: The Plan is not required to agree to your request:**

- **Right to Request Confidential Communications:** Participants have the right to request that the Plan communicate with them about health matters in a certain way or at a certain location. For example, a participant can ask that the Plan send explanation of benefits (EOB) forms about their benefit claims to a specified address.

To request confidential communications, participants must make their request in writing to the Plan Administrator. The Plan will make every attempt to accommodate all reasonable requests. Participant requests must specify how or where they wish to be contacted.

**g. Changes to this Notice:**

The Plan reserves the right to change this notice at any time and to make the revised or changed notice effective for health information the Plan already has about its participants, as well as any information the Plan receives in the future. The Plan will post a copy of the current notice in the Company's Benefits Office at all times.

**h. Complaints:**

If a participant believes their privacy rights under this policy have been violated, they may file a written complaint with the Plan Administrator at the address listed below. Alternatively, the participant may complain to the Secretary of the U.S. Department of Health and Human Services, generally, within 180 days of when the act or omission occurred.

**Note: Participants will not be penalized or retaliated against for filing a complaint.**

**i. Other Uses and Disclosures of Health Information:**

Other uses and disclosures of health information not covered by this notice or by the law that apply to the Plan will be made only with the written authorization of the participant. If a participant authorizes the Plan to use or disclose its PHI, the participant may revoke this authorization in writing at any time. If the participant revokes this authorization, the Plan will no longer use or disclose their PHI for the reasons covered by the written authorization; however, the Plan will not reverse any uses or disclosures already made in reliance of prior authorization.

**j. Contact Information:**

Any questions about this notice should be directed to:

**The MICROS Health Plan Administrator  
c/o MICROS Systems, Inc.  
7031 Columbia Gateway Drive  
Columbia, MD 21046  
(443) 285-6000**

**5. INTERPRETATION**

All questions pertaining to this standard should be directed to the Vice President of Human Resources, the Chief Security Officer, or their designates.

**6. REFERENCE**

None