



# **MICROS Systems, Inc. Enterprise Information Security Policy (MEIP)**

Revision 7.2

**November, 2011**

## Table of Contents

### Overview – Enterprise Information Security Policy/Standards:

<b>I.</b>	<b>Information Security Policy/Standards – Preface.....</b>	<b>5</b>
<b>I.1</b>	<b>Purpose .....</b>	<b>5</b>
<b>I.2</b>	<b>Security Policy Architecture .....</b>	<b>6</b>
<b>I.3</b>	<b>Relation to MICROS Systems, Inc. Policies.....</b>	<b>6</b>
<b>I.4</b>	<b>Interpretation.....</b>	<b>7</b>
<b>I.5</b>	<b>Violations.....</b>	<b>7</b>
<b>I.6</b>	<b>Enforcement.....</b>	<b>7</b>
<b>I.7</b>	<b>Ownership.....</b>	<b>7</b>
<b>I.8</b>	<b>Revisions.....</b>	<b>7</b>
<b>II.</b>	<b>Information Security Policy - Statement.....</b>	<b>8</b>

### MICROS Enterprise Information Security Policy (MEIP):

<b>1.</b>	<b>Information Security Organization Policy (MEIP-001).....</b>	<b>9</b>
<b>2.</b>	<b>Access Management Policy (MEIP-002).....</b>	<b>10</b>
<b>3.</b>	<b>Systems Security Policy (MEIP-003).....</b>	<b>11</b>
<b>4.</b>	<b>Network Security Policy (MEIP-004).....</b>	<b>12</b>

<b>5. Application Security Policy (MEIP-005)</b> .....	<b>13</b>
<b>6. Data Security/Management Policy (MEIP-006)</b> .....	<b>14-15</b>
<b>7. Security Incident Handling Policy (MEIP-007)</b> .....	<b>16</b>
<b>8. Security Operations Policy (MEIP-008)</b> .....	<b>17</b>
<b>9. Personal Information Protection Policy (MEIP-009)</b> .....	<b>18</b>
<b>10. Medical Information Privacy Policy (MEIP-010)</b> .....	<b>19</b>
<b>11. Personnel Security Policy (MEIP-012)</b> .....	<b>20</b>
<b>12. Physical &amp; Environmental Security Policy (MEIP-013)</b> .....	<b>21</b>
<b>13. Business Continuity Management Policy (MEIP-014)</b> .....	<b>22</b>
<b>14. Compliance Policy (MEIP-015)</b> .....	<b>23</b>

## Document History:

<u>Version</u>	<u>Date</u>	<u>Description</u>	<u>Author</u>
2.0	November, 2008	Initial release.	James Walsh
3.0	December, 2008	Update	James Walsh
4.0	December, 2008	Update	James Walsh
5.0	February, 2009	Update	James Walsh
6.0	March , 2009	New sections added. Personal Information and Medical Information.	James Walsh
7.2	November, 2011	Chapter I,II and Policy chapter 11-15 added, reference to ISO27001 added, list of changes added, document number added Security Policy and Standards separated into two documents.	James Walsh; Uwe Maulhardt



## **I. ENTERPRISE INFORMATION SECURITY POLICY/STANDARDS - PREFACE**

### **I.1 PURPOSE**

MICROS Systems, Inc. (MICROS) manufactures sells and services computer-based point-of-sale (POS) and property management systems (PMS) for the global hospitality industry. This includes restaurants, hotels, theme parks, stadiums, casinos, cruise ships, institutional feeding, specialty retail and many other similar global markets. MICROS's services include system planning, acquisition and configuration, on-site and remote installation, on-site and remote support, updates training, hardware service and repairs, spare parts and supplies as well as managed hosting services and software as a service for its customers.

While providing these services, MICROS may sometimes take custody or control of certain non-public sensitive information belonging to its customers. In such cases, MICROS may have a responsibility to protect this sensitive non-public customer information while in its custody or control.

In addition, all employees, contractors, consultants, temporary employees, customers, visitors, vendor personnel or other personnel accessing MICROS owned or controlled IT facilities, networks, information systems, assets or information, (individually and collectively Users), have a responsibility to protect these assets and data, which are vital to the effective operation of our business.

The purpose of the Enterprise Information Security Policy and Standards is to facilitate and promote information security throughout the global company enterprise. The Enterprise Information Security Policy Statement, as shown in Chapter II of this document, describes the company's high level security objectives and is issued to all company employees and other Users. The further chapters of the Policy describe in more detail the security requirements for each specific area.

This Policy applies to all Users accessing or using MICROS Systems, Inc. owned or controlled information technology resources, assets and facilities. This Policy applies to all equipment that is owned or managed by MICROS Systems, Inc. or its subsidiaries and to all third party equipment connected to company owned or controlled business systems.

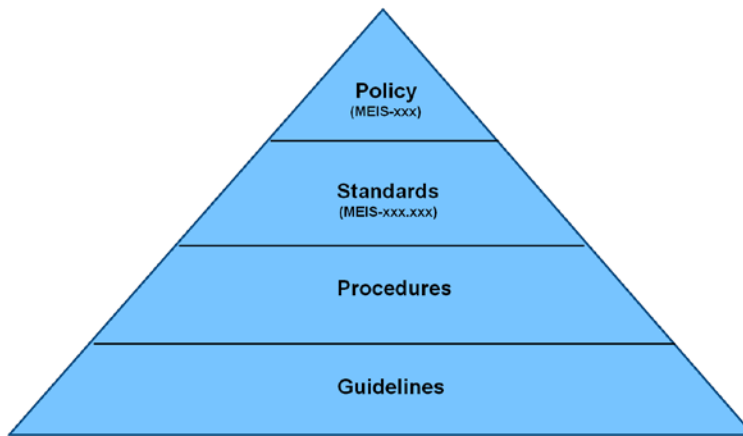


## I.2 SECURITY POLICY/STANDARDS ARCHITECTURE

To facilitate a structured approach to information security, a layered architecture has been defined. The structure and contents of the Policy and Standards are based on an internationally accepted security standard (ISO27001). The framework consists of the following elements:

Security Policies define the goal, the purpose, the scope and responsibilities of the Policy. Security Standards define the minimum requirements for each topic, but in a generic way. Security Policies and Standards are consistent and mandatory worldwide and are maintained by the responsible Chief Security Officer.

Security Procedures and Guidelines are more specific to a particular geographic region, department or market and must, at a minimum, meet the global Enterprise Security Policies and Standards defined herein. Procedures and Guidelines can be stronger than the global Enterprise Policies and Standards. The ongoing maintenance of Procedures and Guidelines are a regional or local responsibility.



## I.3 RELATION TO MICROS SYSTEMS, INC. POLICIES

If there is a conflict between these Policies, and other 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 prevail.



## **I.4 INTERPRETATION**

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

## **I.5 VIOLATIONS**

Any violations of the Policy or Standards may result in disciplinary action, up to and including termination of employment or contract. This document in no way shall be construed to represent a contract of employment between MICROS Systems, Inc. and any Users.

Any User who is requested to undertake an activity which he or she believes is in violation of the Policy or 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.

## **I.6 ENFORCEMENT**

If there is a discovery of violation to the Policy or Standard, the Chief Security Officer or its designate shall be notified in writing as soon as possible.

## **I.7 OWNERSHIP**

The Policies and Standards are owned by the Chief Security Officer. It is the responsibility of the Information Security department to review these Policies and Standards on an annual basis.

## **I.8 REVISIONS**

Within the constraints of applicable law, MICROS Systems, Inc. reserves the right to modify or terminate the Policies and Standards at any time it deems necessary, with or without notice. In the event that a particular Policy or Standard cannot be executed for a specific situation, a statement of risk along with compensating controls shall 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 Policy or Standard based on the statement of risk.



## II. ENTERPRISE INFORMATION SECURITY POLICY STATEMENT

### **Objective:**

The overall objective of information security is to promote business continuity and to mitigate damage caused by the loss or compromise of sensitive non-public information or the disruption of IT infrastructure or services.

### **Purpose:**

The purpose of the MICROS Systems, Inc. Enterprise Information Security Policy (Policy) and Standards (Standards) are to protect MICROS' owned or controlled IT infrastructure and sensitive non-public information assets and the sensitive non-public information assets of its customers, as applicable or contractually committed, from reasonably foreseeable threats, whether internal or external, deliberate or accidental.

### **Scope:**

The Policy and Standards apply 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 (collectively Users). The Policy and Standards apply to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks. The Policy and Standards apply to all Users and to all sensitive non-public information, whether owned by MICROS or in the possession or control of MICROS.

It is the Policy of the company to ensure that:

- Information shall be protected against unauthorized access.
- Confidentiality of Information shall be maintained.
- Integrity of Information shall be maintained.
- Business requirements for availability of Information and systems shall be achieved.
- Risk management assessments shall be performed to identify and evaluate security risks so that appropriate measures can be taken.
- Classification of Information assets shall be applied.
- Country and industry regulatory and legislative, and contractual security requirements shall be achieved.
- Information security awareness training shall be conducted for all Users.
- The responsible Chief Security Officer shall perform the role and responsibility for structuring Information security within MICROS and has direct responsibility for maintaining the global Policies and providing advice and guidance on its implementation.
- Security Procedures and Guidelines must be produced within the company defined geographic regions and locally to support the local implementation of the global enterprise Policies in accordance with local legislation. These local rules define the minimum level of compliance for all Users regarding information security.

All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their Users.

It is the responsibility of all Users to comply with the Policy and related Standards, Procedures and Guidelines.



Non-compliance of these may result in disciplinary action, up to and including termination of employment or contract.

Users should report all breaches of information security, actual or suspected, to their manager or local/regional security officer. In case of a security incident, immediate action must be taken to reduce the risk and impact of damage to MICROS and its clients.

Exceptions to the Policy require the approval of the responsible Chief Security Officer.

## **1. INFORMATION SECURITY ORGANIZATION POLICY (MEIP-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 (Users). 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 or networks.

### **1.3 DEFINITIONS**

None

### **1.4 STATEMENT OF POLICY**

Appropriate organizational capability shall be maintained to create, promote and manage the Information Security policies, standards, procedures and guidelines 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 (MEIP-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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **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 (MEIP-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 non-public 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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

#### **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**

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



## **4. NETWORK SECURITY POLICY (MEIP-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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **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 (MEIP-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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **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 (MEIP-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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **6.3 DEFINITIONS**

**Company Information** -Material non-public information pertaining to the company, confidential information, personally identifying information, financial information, health care 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 (MEIP-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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **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 Users 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 (MEIP-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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### 8.3 DEFINITIONS

**Compromise** – Intrusion into business systems or networks where unauthorized access, disclosure, modification, exfiltration 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





## **10. MEDICAL INFORMATION PRIVACY POLICY (MEIP-010)**

### **10.1 PURPOSE**

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 Policy 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").

### **10.2 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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **10.3 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.

### **10.4 STATEMENT OF POLICY**

All Users who handle, store or have access to PHI must comply with the MICROS Systems, Inc. Medical Information Privacy Standard.

### **10.5 REFERENCE**

-MEIS-010.001 Medical Information Privacy Standard.



## **12. PERSONNEL SECURITY (MEIP-012)**

### **12.1 PURPOSE**

The purpose of this Personnel Security Policy is to ensure that all Users of company owned or controlled information systems or assets containing confidential or sensitive non-public information belonging to MICROS or its customers are aware of, and meet necessary security requirements prior to and during employment.

### **12.2 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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **12.3 DEFINITIONS**

None

### **12.4 STATEMENT OF POLICY**

All Users who have access to MICROS's information or assets or to sensitive non-public customer-owned information or assets must comply with MICROS Systems Inc. Personnel Security Standard

### **12.5 REFERENCE**

-MEIS-012.001 Personnel Security Standard



## **13. PHYSICAL & ENVIRONMENTAL SECURITY POLICY (MEIP-013)**

### **13.1 PURPOSE**

MICROS' computing and networking areas are operated as closed facilities with controlled access to authorized personnel only. A process for access control and authorization must be in place. The purpose of this Physical & Environmental Security Policy is to ensure that all Company owned or controlled computing and networking areas shall be physically protected from security threats and risks from environmental threats and hazards such as fire and smoke damage, water flooding, power failures, humidity problems, lightning, technical malfunctions, sabotage and theft.

### **13.2 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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **13.3 DEFINITIONS**

None

### **13.4 STATEMENT OF POLICY**

All Company owned or controlled facilities and computing and networking areas must comply with the MICROS Systems Inc. Physical & Environmental Security Standard.

### **13.5 REFERENCE**

-MEIS-013.001 Physical & Environmental Security Standard



## **14. BUSINESS CONTINUITY MANAGEMENT POLICY (MEIP-014)**

### **14.1 PURPOSE**

The purpose of this Business Continuity Management Policy is to ensure that MICROS is able to minimize the business impact of any unplanned disruptions or outages of its systems or operations and to be able to resume disrupted services or activities as quickly as possible.

### **14.2 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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **14.3 DEFINITIONS**

**Business Continuity Management (BCM):** Ensures the continuation or the timely resumption of business processes in case of a disruption.

**Business Impact Analysis (BIA):** Assessment of the risks to business processes in case of a partial or full outage.

### **14.4 STATEMENT OF POLICY**

All Users and departments responsible for critical Company business processes and assets must comply with the MICROS Systems Inc. Business Continuity Management Standard.

### **14.5 REFERENCE**

-MEIS-014.001 Business Continuity Management Standard



## **15. COMPLIANCE POLICY (MEIP-015)**

### **15.1 PURPOSE**

The purpose of this Compliance Policy is to ensure that Company owned or controlled facilities, networks, systems, applications and information comply with MICROS' Security Policy & Standards, contractual agreements, relevant laws and industry standards and other requirements. Controls must be in place to ensure compliance with these requirements and standards. Compliance must be periodically reviewed. Noncompliance must be promptly reported to responsible management personnel. Management must then ensure that timely, appropriate and auditable action is taken to resolve any instances of noncompliance.

### **15.2 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 (individually and collectively Users). This policy applies to all information technology facilities, systems and networks that are owned or leased and controlled by MICROS Systems, Inc. and to all third party equipment connected to any such facilities, systems or networks.

### **15.3 DEFINITIONS**

None

### **15.4 STATEMENT OF POLICY**

All Users who have access to MICROS's information or assets or to sensitive non-public customer-owned information or assets must comply with MICROS Systems Inc. Compliance Policies and Standards.

### **15.5 REFERENCE**

-MEIS-015.001 Compliance Standard