Information Security Policy

Euronet Services India Pvt. Ltd.
Lodha I-Think Techno Campus,
Office No. 1, 8th Floor, Wing “A”,
Off. Pokhran Road No. 2
Behind TCS, Eastern Express Highway,
Thane, India - 400 607
Phone Number: +91 – 22 – 3939 7000
Fax Number: +91 – 22 – 3939 7239

Document Control

Document Reference		EN/ISMS/A.5.1/ISP/POL/V 3.4			
Document Description		Information Security Policy			
Document Owner		Information Security Officer			
Department		Audit and Compliance			
Version No.	**Date**	**Status**	**Changes Made**	**Author**	**Initialed**
1.0	24/02/2006	Final	–	Information Security Officer	
1.1	28/04/2006	Final	Grammatical changes were made. Management Policies list was added	Information Security Officer	
2.0	27/08/2007	Final	Classification changed to internal	Information Security Officer	
2.1	16/04/2008	Final	Changes have been recorded and approved in ISMF meeting	Information Security Officer	
3.0	12/03/2009	Final	Changes have been made to meet the PCI DSS requirements	Information Security Officer	
3.1	30/12/2009	Final	Points added 6.xxiii - 6.xxvi	Information Security Officer	
3.1	25/06/2010	Final	No changes were made	Information Security Officer	
3.2	01/04/2011	Final	Changes made – Please refer the ISMS Policy & Procedure Change Tracker	Information Security Officer	
3.3	01/06/2012	Final	Changes made – Please refer the ISMS Policy & Procedure Change Tracker	Information Security Officer	
3.4	06/06/2013	Final	Changes made – Please refer the ISMS Policy & Procedure Change Tracker	Information Security Officer	

Table of Contents

Contents

1. Introduction 3
2. Policy Objectives.....3
3. Scope.....3
4. Roles and Responsibilities.....4
5. Security Incidents 4
6. Information Security Policy Rules 5
7. Review of Information Security Policy 6
8. Supporting Policies.....6

1. Introduction

Information is one of a Euronet's most important assets. Protection of information assets is necessary to establish and maintain trust between the Euronet and its customers. Timely and reliable information is necessary to process transactions. Euronet's earnings and capital can be adversely affected if this information becomes available to unauthorized parties or is altered or is not available when it is needed.

Information security management is the process by which Euronet Services India Pvt. Ltd. protects and secures information resources that process and maintain information vital to its operations.

Euronet Services India Pvt. Ltd. will measure, manage and control the risks to systems and ensure data availability, integrity, confidentiality and accountability for system actions.

2. Policy Objectives

The purpose of information security management is to protect the information resources of Euronet from unauthorized access or damage. The securing of Information resources will be to achieve

- **Information Resource Availability** — The information resources of Euronet, including the network, hardware, software, facilities, infrastructure, and any other such resources, are available to support Euronet business objectives.

- **Data Integrity** – The data used in the information systems at Euronet can be trusted to correctly reflect the reality it represents. The ability to access or modify data is provided only to authorized users for authorized purposes

- **Data Confidentiality** – All applicable users of Euronet data and IT resources are responsible for confidentiality of any information shared verbally or viewed via IT resources.

3. Scope

This policy applies to all users of information assets including current employees, employees of temporary employment agencies and contractor/third party service provider personnel. Every user of any of Euronet's information resources has some responsibility toward the protection of those assets; some departments and individuals have very specific responsibilities.

This policy refers to all information resources whether individually-controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by Euronet. This includes but is not limited to networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, minicomputers, and any associated peripherals and software.

4. Roles and Responsibilities

Information security is the responsibility of everyone in Euronet Services India Pvt. Ltd., as well as the Euronet's service providers and contractors. The management and employees all have different roles in developing and implementing an effective security process.

i. **Information Security Management Forum (ISMF)** – An Information Security Forum will be in place to ensure clear direction and visible management support for security initiatives within Euronet Services India Pvt. Ltd. To represent ISMF, Management Representative will be appointed
ii. **Information Security Officer (ISO)** — The Information Security Officer is responsible for providing interpretation of this and other related policies and disseminating related information
iii. **System and Data Owners** — System and data owners are responsible for the application of the policies relating to the systems, data, and other information resources under their care or control
iv. **System Administrators** — System administrators are responsible for the application of the policies relating to the systems, data, user access rights, and other information resources in their care at the direction of the system and data owners. System Administrators are also responsible for implementing strong password controls on all IT systems, applications, and peripheral IT systems.
v. **Network Administrators** — Network administrators are responsible for the application of the policies relating to the communication systems (i.e., network and telecommunications security, routers, WAN security, etc.). This includes ensuring that all IT network resources are protected from unauthorized access, initiating corrective measures and reporting security breaches.
vi. **Information Security Audit Team** — The ISA Team shall conduct the ISMS audit at planned intervals with prior permission of the ISMF. The Internal audit team shall submit a report on findings and opinions on the periodic reviews with the required improvements.
vii. **Incident Response Team** — The Incident Management Team shall ensure that whenever a security incident is suspected or confirmed, the appropriate Incident Management procedures must be followed. All incidents – of any type – should be recorded, reviewed and resolved using an incident management process. The Incident Response Team should follow a formal documented method for reporting incidents to the ISMF.
viii. **Business Continuity and Disaster Recovery Team** — The BCP and DRP team shall ensure continuity of business processes in the event of planned or unplanned outages and recovery to normal operations with least efforts in shortest time possible.

5. Security Incidents

All Euronet India employees and applicable users noted above are responsible for reporting any security incident to the Information Security Officer or to a member of Information Security Management Forum (ISMF).

The details of the security incident will be kept confidential and will be investigated by the individual who the incident was reported through. Appropriate action will be taken to address each security incident on a case-by-case basis.

6. Information Security Policy Rules

i. Appropriate protection for all organizational assets by accounting for and nominating an owner for all major assets.
ii. The risks associated with all organizational assets will be identified and continuously monitored. This will be done on annual basis and a report will be submitted to the ISMF for approval of the identified risks.
iii. All information assets will be classified as CONFIDENTIAL or INTERNAL or PUBLIC.
iv. Employees, contractors and third party users should understand their responsibilities. They should be suitable for their roles to reduce the risk of theft, fraud or misuse.
v. Appropriate mechanisms will be in place to prevent unauthorized physical access, damage and interference to business premises and information
vi. Equipments should be protected from physical security threats and environmental hazards
vii. Policies and procedures will be in place to minimize the risk of system failures, by ensuring availability of adequate capacity and resources
viii. Tools and mechanisms will be in place to protect the integrity of software, applications and information, by preventing and detecting the introduction of malicious software
ix. Access to information and business processes will be based on business and security requirements
x. Cryptographic systems and techniques will be used for the protection of key information that faces a high risk of tampering or disclosure
xi. Consistent and effective approach will be applied to the management of information security incidents
xii. Preventive and recovery controls will be put in place to counteract interruptions to business activities and protect critical business processes from major failures of information systems or disasters
xiii. The security of information systems will be regularly reviewed. Such reviews will be performed against the appropriate security policies
xiv. Technical vulnerabilities will be assessed on regular intervals
xv. Non disclosure agreements will be signed with all concerned persons (employees / third party contractors) who access ESIL resources and information.
xvi. Contacts with statutory, regulatory, legal bodies and emergency services will be maintained
xvii. Contacts with security forums and security consultants will be maintained
xviii. All changes to the ISMS documents shall be made with approval from ISMF members
xix. Contact with special interest group for information Security shall be maintained
xx. Daily operational security procedures are drafted and is consistent with administrative and technical procedures
xxi. Assist in creation and distribution of security policies / procedures will be done by the ISO
xxii. Proper due diligence will be conducted prior to engaging any service provider
xxiii. Euronet shall comply with all relevant laws having bearing on information security
xxiv. Euronet shall retain and protect all records and information for the period required by relevant legislations and/or statutory bodies
xxv. Euronet shall ensure access to system audit tools are allowed only to authorized users and for the purpose of conducting audits
xxvi. Euronet shall ensure secure maintenance of adequate evidence as required under the relevant laws and / or internal policies and procedures

7. Review of Information Security Policy

This policy will come into effect after review and approval of the Information Security Management Forum (ISMF) of Euronet Services India Pvt. Ltd. The ISMF of Euronet Services India Pvt. Ltd. is the owner of the Information Security Policy and any changes to the same have to be authorized by the Forum members.
The security policy will be reviewed on annual basis or any major changes to business objectives.

8. Supporting Policies

Management Polices and Guidelines

i. Policy for Control of Documents and Records
ii. Policy for ISMS Improvement
iii. Policy for Management Responsibility
iv. Policy for Management Review of ISMS
v. Policy for Information Risk Management
vi. Risk Assessment Guidelines
vii. Risk Mitigation Guidelines

ISMS Policies

i. Policy for Information Security Organization
ii. Policy for Management of Information Processing Facilities
iii. Policy for Asset Management
iv. Policy for IT Acceptable Usage
v. Policy for Third Party Connection
vi. Policy for Physical and Environmental Controls
vii. Policy for Communication and Operations Management
viii. Policy for Malicious Software
ix. Policy for Network Security Management
x. Policy for Media Handling and Security
xi. Policy for Exchange of information
xii. Policy for Access control
xiii. Policy for User access and password management
xiv. Policy for Operating System Access Control
xv. Policy for Application and Information access control
xvi. Policy for Information systems acquisition, development and maintenance
xvii. Policy for Mobile computing
xviii. Policy for Incident Management
xix. Policy for Business Continuity Management
xx. Policy for Email usage
xxi. Policy for Clear Desk and Clear Screen
xxii. Policy for Firewall Management
xxiii. Policy for Card Information Access and Storage
xxiv. Policy for Customer Data Protection
xxv. Policy for Key Management
xxvi. Euronet India HR Policies