Edenred Finland Oy - Security description 30.03.2018

INTRODUCTION

1. Preface

In today's society data, or information, is everywhere. Sensitive personal and business information falling into the wrong hands can cause substantial damage financial and otherwise, and therefore the protection of information is of the utmost importance.

2. About information security at Edenred

Edenred Finland's information systems – Ticket on the Web, MyEdenred and the Affiliate portal – have been placed ISO/IEC 27001:2013 certified data centers, which ensures that information is usable when needed and only by authorized entities.

The payment transactions, cardholder data and associated systems used by Edenred Finland's applications are secured by PCI DSS certified solutions, including the use of secure networks and strong access control measures.

On all other information security related matters ISO/IEC 27001:2013 and the controls defined by it are used as a reference framework and a target level for security practices and procedures in risk assessment and mitigation.

Edenred employs a large, professional information security team organized around areas including infrastructure and architecture, security intelligence and crisis management, and application security.

3. About this document

This document provides information on the overall security policies, standards, procedures and best practices for the applications/services implemented and maintained by Edenred. It is designed to help Edenred's customers to find, address or clarify any relevant security information in doubt.

The primary audience for this document are the information technology as well as information security professionals in Edenred's customers' organizations.

4. About ISO/IEC 27001 and PCI DSS

ISO/IEC 27001 is the best-known standard for defining and Information Security Management System or ISMS. Its purpose is to ensure the security of an organization's information assets by preserving their confidentiality, integrity and availability by applying a risk management process.

PCI DSS (Payment Card Industry Data Security Standard) is the global data security standard adopted by the payment card brands, such as MasterCard and Visa, for all entities that process, store or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data.

Contents

5. Organization of Information Security

Edenred has defined information security responsibilities and duties regarding the services provided to their customers.

Edenred shall use skilled professionals in a safely organized manner and in accordance with good practices.

Edenred has appointed a manager responsible for implementing and maintaining security in their services and environments.

Edenred's security related activities cover the following responsibilities:

- Assignment of Edenred's security resources;
- Interfacing with customers on all security requirements; and
- Implementing the security requirements.

5.1. Employees

Edenred's employees shall report all identified information security weaknesses, actual and suspected security breaches related to the services provided to their customers to their immediate manager or the defined security organization. The security organization is responsible for further reporting to customers if the security event affects or targets their information.

5.2. Information security in project management

Edenred addresses information security in all projects starting from project initiation and maintains it through the project life cycle and transition to operation. This applies to all projects related to the services provided to Edenred's customers.

Information security is generally integrated into Edenred's project management methods in order to identify and address information security risks as part of services provided to their customers. This includes an information security risk assessment in an early stage of the project to identify necessary controls.

5.3. Human resource security

Edenred performs background verification checks on its employees that may access, process, store, and/or communicate information assets as part of the delivery of services to their customers.

Edenred provides initial and regular awareness training for all its employees involved in the delivery of services to their customers. This training includes information of common threats and vulnerabilities related to information security, as well as information on personal responsibilities in handling and protecting information assets.

6. Asset Management

Edenred retains an inventory of all IT assets involved in the delivery of services towards their customers. The inventory holds information about each IT asset. Any changes to IT assets are implemented through a structured process.

6.1. Securing IT assets before disposal

Edenred handles the disposal of IT assets, such as storage media like hard disks on PC's and licensed software, according to a defined process, which has a defined process owner. Worn out physical IT assets shall neither be stored freely accessible nor be sold or disposed of, before the data stored on the IT assets has been deleted and cannot be recreated.

6.2. Handling of IT assets and information assets

Edenred uses appropriate precautions to secure IT assets and information assets used in the delivery of services to their customers, against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

Information assets are shared only with individuals with a direct individual work-related need.

6.3. Media handling

Removable media is any device or media that can hold information. Removable media includes but is not limited to tapes, disks and printed media.

Media with any sensitive or customer data is physically protected and Edenred has appropriate handling procedures to protect information on removable media from unauthorized disclosure, modification, removal, and destruction.

USB flash drives will not be used to store Edenred's customers' data.

6.4. Disposal of data

During the term of the agreement if there is no need for Edenred to keep customer data or at the termination of the agreement, Edenred shall return or destroy any and all of that specific customer's data.

Edenred utilizes good industry practices to dispose customer data such as clear, purge or destroy to achieve the results required.

7. ACCESS CONTROL

7.1. Access control

Assigning of access rights to information and IT systems for Edenred's employees are in accordance with the users role description/job function relating to the services delivered. Access to customer information shall be granted only to authenticated and authorized users on a need-to-know basis.

Edenred's employees shall only access data through management tools providing traceability and not bypassing authorization controls. In the event of a system failure or if the access control mechanism is malfunctioning, access must be denied by default.

7.2. Access management

7.2.1 User administration

All Edenred's employees, including operations personnel, network administrators, system engineers, database administrators etc. shall be given a unique user ID, which they are personally responsible for. Authorizations for the user ID's are in compliance with users' role description/job function.

7.2.2 Password management

Before access is given the user shall be authenticated. For logon to Edenred's systems a password is used to verify the user's identity and thereby his/her rights to access information and permission to use the system. Additional authentication mechanisms, such as two-step authentication is used when stronger authentication is required.

Passwords are required to comply with industry best practices regarding complexity.

Passwords are not shared with third parties nor will they be transmitted in clear text across unsecure networks. Stored passwords shall be encrypted.

7.2.3 Review of user access rights

Edenred's employees shall be allocated access rights after "least privilege" principle, meaning only enough rights for the execution of their defined work tasks.

All access rights shall be reviewed on a regular basis by Edenred. User IDs with privileged access rights shall not be used for ordinary office work, but only for the approved purpose.

7.2.4 Clear desk and clear screen policy

Edenred's employees are instructed to lock away any sensitive information, such as system documentation or data on electronic storage media, when the information is not needed. Information shall be placed in a way that unauthorized access is restricted.

Edenred's employees are instructed to log off or lock systems when leaving the computer or alike. Time-out procedures are used for both users and for remote connections, which automatically terminates the session if there is no activity.

7.3. Mobile devices

Mobile devices such as smartphones, tablets and laptops are required to have sufficient security measures in use to prevent unauthorized access. Mobile devices that are not managed by Edenred are only allowed limited access to any Edenred network and will only be allowed to connect for a predefined amount of time. Mobile devices (excluding Edenred owned laptops in the Edenred domain and network) are not granted access to sensitive customer, personal or operational information.

8. Cryptography

Edenred uses cryptographic controls to protect the confidentiality, authenticity and integrity of information when stored or transferred outside Edenred controlled networks. Information is encrypted at all times when data is transferred.

Passwords and other means of authentication, by which users can logon and get access to perform transactions, shall be protected from eavesdropping through encryption.

When Cryptographic solutions are used, only acknowledged algorithms and recommended key length is used.

9. Physical and environmental Security

Edenred shall protect their customers' information and IT equipment with physical and environmental security.

9.1. Secure areas

Edenred's customers' information and IT equipment storing that information shall be placed in secure areas to prevent unauthorized physical access, damage and interference.

9.1.1 Responsibilities

For "secure areas" such as data centers, computer rooms, technical rooms or cabinets hosting IT equipment placed at Edenred, an IT area owner is appointed.

9.1.2 Physical security perimeters

Security perimeters are defined and used to protect areas that contain either sensitive or critical information or information processing facilities, from loss, theft, damage, interference, interruption, or unauthorized physical access.

9.1.3 Physical entry controls

Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access;

- The date and time of entry and departure of visitors is recorded, and all visitors are supervised unless their access has been previously approved; they are only be granted access for specific, authorized purposes and are issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors is authenticated by an appropriate means.
- Access to areas where confidential information is processed or stored is restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN;
- Physical log book or electronic audit trail of all access is securely maintained and monitored;
- All employees, contractors and external parties are required to wear some form of visible identification and notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
- External party support service personnel are granted restricted access to secure areas or confidential information processing facilities only when required; this access is authorized and monitored;
- Access rights to secure areas are regularly reviewed and updated, and revoked when necessary

9.1.4 Securing offices

Edenred ensures that offices with workstations used for providing services to their customers shall be guarded by sufficient perimeter access control as well as intrusion and fire detection. All premises or buildings shall have an audible alarm system as well as a connection to an emergency service center.

Windows and doors, which can be forced from the ground floor, are equipped with sufficient physical security controls. Appropriate precautions have been taken to secure Edenred's customers' information against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

9.1.5 Hazard protection

Edenred ensures that IT facilities used to provide services to their customers shall be located in a safe environment protected from natural and man-made hazards, i.e. as flooding, fire or damage from neighboring activities. Operational systems run in two different data centres located at a sufficient geographical distance from each other. An offsite back-up of information is stored at a separate location. The data centres are not dependent on the same physical infrastructure.

9.2. Equipment security

9.2.1 Supporting utilities

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning):

- Conform to equipment manufacturer's specifications and local legal requirements;
- Appraise regularly for their capacity to meet business growth and interactions with other
- Supporting utilities;
- Are inspected and tested regularly to ensure their proper functioning;
- Are alarmed to detect malfunctions;
- Have multiple feeds with diverse physical routing.

Emergency lighting and communications are provided. Emergency switches and valves to cut off power, water, gas or other utilities are located near emergency exits or equipment rooms.

9.2.2 Cabling security

Power and telecommunications cables/lines in the data centre are placed underground, where possible, or subject to adequate alternative protection. Power cables shall be segregated from communications cables to prevent interference.

9.2.3 Security of equipment and assets off-premises

The use of any information storing and processing equipment outside Edenred's premises must be authorized by management at any time. This applies to all equipment at any time owned by Edenred as well as equipment owned privately and used on behalf of the organization.

10. Operations Security

Operations security describes requirements for stability, monitoring and security related to the daily operations of information systems.

10.1. Separation of development, test and operational environments

Edenred maintains a clear logical separation of all development, test and production environments in order to prevent unauthorized access or changes in the production environment. Development and test systems are hosted on network segments separated from production network, using a virtual local area network and firewalls.

Separation of environments shall be supported by a clear naming standard, logical access control and physical separation.

10.2. Operating procedures

Edenred ensures the existence of up-to-date documentation with relevant information relating to the operational activities associated with systems, including but not limited to back-up procedure and handling, contact information for technical support and relevant stakeholders, etc.

10.3. Change Management

All changes to business applications, computer systems and networks are performed in accordance with a change management process, which comprises the process from the recording of a change to the review after implementation into production.

The change management procedure requires that before a change is applied to the operational environment, the following tasks are performed:

- identification and recording of the change in a change register to ensure tracking of the change from its approval through to closure;
- assessment of the potential impacts of such changes;
- adequate testing of the change,
- accurate version control; and
- fall-back plan for aborting and recovering from unsuccessful changes.

All changes are documented according to the above and logged to change register.

The implementation of changes, also called release management, shall be documented and controlled to minimize any negative effects on the production environment.

10.4. System planning and acceptance

10.4.1 Capacity management

Capacity requirements are identified, taking into account the business criticality of the concerned system. System tuning and monitoring is applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls are in place to indicate problems in due time. Projections of future capacity requirements are taken in account of new business and system requirements and current and projected trends in the organization's information processing capabilities. Spare parts are available for mission critical systems.

10.4.2 System acceptance

Edenred uses a formal approval process (system acceptance) to ensure that acceptance criteria for new or significantly-changed applications are established and that suitable tests of the systems are performed during development and prior to implementation. These acceptance criteria include but are not limited to:

- agreed security controls in place;
- evidence that installation of a new system has no adverse effects on existing production systems; and
- Compliance with performance and capacity requirements.

10.5. System management

System management refers to design and administration of infrastructure, applications and network management.

10.5.1 Computer and network installations and design

Edenred ensures that an up-to-date documentation for computer system, network, firewall and telecommunication installation designs exists.

Edenred ensures the implementation of designs that minimize manual intervention by incorporating high-reliability systems designed around the concepts of fault tolerance, patch management, and automated back-up that can be remotely configured and automatically monitored against predefined thresholds.

Administrative access to computer systems, network devices, firewalls and telecommunications equipment is built with security by design. Strong security controls and surveillance, as well as intrusion detection sensors are in place.

10.5.2 Server Configuration

All Edenred's physical and virtual servers have a standard configuration which includes descriptions of disabling/restricting of unnecessary functions or services.

Each server is also protected by applying standard security management practices (including restricting physical access, system hardening, applying change management and malware protection, monitoring and performing regular reviews, and applying network-based security controls, such as firewalls and intrusion detection.

Access to powerful system utilities and server parameter settings is authorized and restricted to a limited number of individuals.

10.5.3 Virtual Servers

Edenred's virtual servers are deployed on robust, secure physical servers and configured to protect information. Physical servers that are used to host virtual servers are protected against unmanaged and ad hoc deployment of virtual servers, as well as resource overloads (e.g. excessive use of the CPU, memory, hard disk and network).

10.6. Monitoring and logging

Procedures for monitoring the use of Edenred's information systems are established using event logging and automated monitoring systems capable of generating consolidated reports and alerts on system security.

Logs are stored for at least 12 month in a secure environment and only accessible for authorized personnel only.

10.7. Technical Vulnerability Management

Edenred gathers information about, and assesses software vulnerabilities, by utilizing all relevant available sources like mailing lists, websites, suppliers and other contacts/networks. The timely receipt and review of technical vulnerabilities related to information systems in use is implemented to ensure that Edenred's exposure to such vulnerabilities is evaluated and appropriate measures are taken to address the risk.

Vulnerability management shall comprise all platforms that contain sensitive, confidential or customer information, such as servers, workstations, laptops, mobile devices, network devices, firewalls and any other components with embedded software connected to Edenred's network.

Edenred shall ensure that software used in operational systems is supported.

10.7.1 Vulnerability scanning and security patch management

All Edenred's IT Systems are regularly scanned for vulnerabilities. Identified vulnerabilities are mitigated by installing relevant security patches or performing other mitigating actions.

All security patches are evaluated on their relevance and urgency. The risks posed by the vulnerability is compared with the risk of installing the security patch.

10.7.2 Protection from Malware

Anti-virus and anti-malware solutions are installed on applicable systems and regularly updated to protect against threats, such as viruses, worms, Trojan horses, etc. This is complemented with awareness advice for users.

10.7.3 Restrictions on software installation

Local administrator rights shall be approved by a manager and may be given to a user only when strictly necessary.

Prior to installation of software on IT systems, there must be an evaluation performed to ensure that it does not violate regulatory or legal obligations or disrupt normal operations.

Edenred does not allow installing unauthorized and/or illegal copies of software on their computing environment.

10.8. Back-up

Back-ups are performed for all Edenred's systems, information and data including operating system, system software, system documentation, data, software and licenses. Back-ups are regularly tested to ensure that they can be read and restored when needed.

Access to the back-up media is restricted to only authorized personnel.

All Edenred's systems use highly redundant servers as a first protection against loss of information. Back-ups of data are done on SAN and tape according to a predefined schedule. Back-ups on removable media are encrypted and stored on a physical separated location.

11. Communications Security

Edenred's networks and its supporting information processing facilities are protected against the compromise of confidentiality, integrity and availability of the information they process.

11.1. Network Security Management

Edenred's network and telecommunication installations are able to cope with current and predicted load, quality and availability requirements, and protected against internal and external threats using a range of security controls such as security rules, policies, hardware and applications.

11.2. Network Device Configuration

Network infrastructure devices, including but not limited to routers, switches and firewalls in Edenred's network are configured to function as required and to prevent unauthorized or incorrect updates. Network devices are subject to standard security management practices, which include:

- restricting physical access to network devices by locating them in secure or dedicated, locked storage rooms;
- 'hardening' the operating system(s) that support them i.e. disabling unnecessary services and changing suppliers' default parameters;
- keeping network devices up-to-date, i.e. by applying security and software updates; and
- Continuously monitoring network devices.

Networks are protected using access control providing differentiated access to networks depending on level of authentication of user and device.

Unauthorized devices are prevented from connecting to or interfering with authorized devices on Edenred's network.

11.2.1 Firewall

Access to Edenred's network is routed through a securely configured firewall prior to being allowed access to internal networks, or before leaving internal networks.

All traffic to and from the firewall is blocked unless specifically authorized.

11.2.2 Proxy

To further increase security in all parts of its network, Edenred has implemented multiple internet proxy solutions that filter users and applications accesses to Internet.

11.2.3 E-mail

Edenred shall not distribute or exchange any customer information externally using e-mail services without encryption. Instant Messaging will not be used for exchange of customer information.

Mail gateways are established to ensure the protection of e-mail from threats such as malware, phishing, etc.

12. Information Systems Acquisition, Development and Maintenance

Necessary security requirements are specified at all system development stages incl. maintenance and decommissioning. The security requirements are both part of the system development at an early stage and considered during the entire system development lifecycle.

12.1. System development security requirements and design

Edenred only uses documented international system development methodologies. These include standards and procedures for developing systems or integrating other systems. The methodologies cover specification of requirements, system design, development, testing and deployment.

Specification of security requirements are documented before the design commences, but can be updated during the development. The system design includes integration of a security architecture that supports the above mentioned requirements as well as the confidentiality, integrity and availability of information.

Validation checks are incorporated into the design of applications to detect any corruption of information through processing errors, human mistakes or deliberate acts.

12.1.1 System Testing and security review

Edenred uses a process for testing systems under development, which is supported by documented supplier standards. This requires that all key components of new systems are tested before deployment to production environment, including application software packages, system software, hardware and communications. No system is allowed to achieve production status, before it has been thoroughly tested. Systems having external connections shall also pass penetration tests.

Vulnerability scan is performed for all systems in all environments. Application security testing is mandatory for all externally reachable applications and interfaces as well as for all systems handling strictly confidential information.

Risks and vulnerabilities identified during these tests are documented and managed. Identified risks are addressed as soon as possible and any residual risks are tracked and followed up.

12.1.2 Security of source code, system files, and operational software

Access to version control system; e.g. system files, source code, designs and specifications are restricted, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

Program source code is not held in operational systems. Program source code is stored centrally in a version control system, which is managed according to established procedures.

12.1.3 Secure development environment

Edenred performs system development activities in appropriately protected secure development environments, which are isolated from the live and testing environments, and protected against unauthorized access.

Edenred performs changes to business applications (including those under development) in accordance with a documented change management process to ensure that they do not adversely affect intended functionality or compromise security controls.

Application source code is protected by removing unnecessary sensitive information from programs, and Malware detection / protection mechanisms are employed prior to deploying them in the live environment.

12.2. Acquisition of Hardware and Software

Software licensing requirements are met by obtaining adequate licenses for planned use and by providing proof of ownership of software.

Hardware and software are acquired from affiliates with a proven record of providing robust and resilient products which shall be tested prior to use.

13. Supplier relationships

13.1. Supplier service delivery management

Edenred regularly monitors and reviews services provided by sub-contractors to verify that the agreed level and conditions of service deliveries and information security are maintained. Appropriate action shall be taken when deficiencies in the service delivery are observed.

Regular monitoring and review of the sub-contractors services shall verify that the terms and conditions of the agreement are being adhered to and that information security Incidents and problems are managed properly.

14. Information security incident management

Information security incidents are managed according to a defined process with the purpose of identifying and responding to incidents and to restore normal status of information/IT systems while minimizing the adverse impact and reducing the risk of similar Incidents occurring.

14.1. Incident management

Reported Incidents are investigated and diagnosed to assess how the incidents are best resolved. Solutions or workarounds and other relevant information about the Incident handling is documented before the Incident record is closed.

Edenred shall report any significant security incidents, which affects the service to their customers without undue delay after the incident is first observed and categorized.

14.2. Problem Management

A problem is an undiagnosed root cause of one or more incidents. Problem management shall be considered for all severe incidents or incidents with high resource consumption in order to produce corrective or preferably preventative solutions.

15. Compliance

Edenred shall comply with information security requirements described in this security description, applicable laws and contractual controls.

15.1. Compliance review

Edenred performs a self-audit on a yearly basis relating to information security requirements. A risk assessment including procedures for identifying, qualifying and mitigating risks is the base of the audit. If any non-compliance is found as a result of the review, Edenred shall evaluate the need for corrective actions and document the result, as well as develop a remediation plan and carry out the remediating actions required to achieve a satisfactory resolution of the respective control deficiency.

The Privacy Policy provides the personal data handling information required by the applicable data protection legislation. The latest document is available in Edenred.fi.