Instant Systems Security Policy

Table of Contents

Introduction

The purpose of this document is to define and acknowledge Instant Systems Sweden AB and its policies and procedures. It should be used by Instant Systems and its PCI DSS partners for the intent of PCI Compliance. It should also be a guideline for the employees regarding the systems in place. The content is based on all the necessary policies and procedures that is needed for PCI compliance and on how to configure the systems in a working and secure way. The document is divided into chapters and every chapter should have a timestamp on when it was last modified. Instant Systems Security Policy should also contain a "Document History" with release version, date, reason for change, status and distribution.

Glossary

ISP	Instant Systems Security Policy
Secure Zone	In-scope credit card environment
DIA	Director of Information Assurance (Security officer)
ROC	Report on Compliance
POS	Point of sale
IRP	Incident Response Plan

See also Official PCI Security Standards glossary

Instant Systems Security Policy

DOCUMENT HISTORY

Release	Date	Reason for change	Status	Changed by
Draft 0.1	2007-12-04	Initial draft	First preliminary draft	Instant Systems
Draft 0.5	2008-02-14	Adapted for Instant Systems	Preliminary draft, adherence to PCI requirements uncompleted	Instant Systems
Draft 0.9	2008-02-15	PCI requirements adherence	PCI requirements checked	Instant Systems
Final 1.0	2008.02.26	Full pci requirements adherence	PCI requirements added	Instant Systems
Final 1.1	2008-02-27	Document restructure	All PCI requirements added	Instant Systems
Draft 1.2	2009-04-28	PCI 1.2 requirements adherence	PCI 1.2 requirements added	Instant Systems
Draft 1.3	2010-05-10	Yearly revision	Fixed language, company name and contact information	Instant Systems
Draft 1.3b	2010-06-21	PCI requirements adherence	Updated the requirements	Instant Systems
Draft 1.4	2010.06.21	PCI requirements adherence	Minor policy changes	Instant Systems
Draft 1.5	2015-09-18	PCI requirements adherence	Updated the requirements for PCI 3.1	Instant Systems
Draft 1.6	2015-09-21	Minor policy change	Updated PCI 5.1	Instant Systems
Draft 1.7	2016-04-11	Policy update	Added desc to PCI 3.0	Instant Systems
Draft 1.8	2017-05-15	Policy update	Annually minor updates	Instant Systems
Draft 1.8b	2017-06-30	Minor changes	Fixed changed/wrong req numbers	Instant Systems
Draft 1.9	2018-05-23	Policy update and changes	Updated the requirements for PCI 3.2	Instant Systems
Draft 1.9b	2018-06-18	Yearly Revision	Minor fixes	Instant Systems
Draft 1.9c	2019-03-19	Minor changes	Change some information about responsibility	Instant Systems
Version 2.0	2019-05-27	Changed policy	Policy 4.3 changed for compliance	Instant Systems
Draft 2.1a	2020-01-09	Minor changes	Clarified policies(1.1.5, 1.3.3, 2.1, 9.1)	Instant Systems
Draft 2.1b	2021-06-21	Minor changes	Clarified policies(1.1.5, 1.3.3, 5.1.1, 9.1)	Instant Systems
Draft 2.1c	2022-03-22	Minor changes	Clarified policies (1.1.1, 9.1)	Instant Systems
Version 3.0	2024-05-13	Changed policy	Server replacement	Instant Systems
Version 3.1	2024-09-25	Changed policy	Server replacement	Instant Systems

Version 3.2	2025-05-05	Yearly Revision	Minor fixes	Charles Carlsson
Version 3.3	2025-06-04	Minor changes	Clarified policy 2.2.4	Charles Carlsson

Executive Summary

Information and information processing resources at Instant Systems are valuable corporate assets. The purpose of information assurance is to ensure the development and implementation of cost effective controls that prevent unauthorized access, modification, destruction or disclosure of division data at any level and to provide the ability to recover information or information processing capabilities. This Instant Systems Security Policy describes the high-level security policy statements that govern the security performance and concerns of Instant Systems in terms of intranet, local network, extranet, key servers and desktop computing devices. The security policy statements contained in this document will be satisfied by execution of security policy enforcement mechanisms that will be implemented by automated or manual means. Actual implementation strategies, countermeasures, and security procedures will be the focus of supporting procedures and guideline documents. This policy is deemed critical for Instant Systems information asset protection and the company's adherence to the PCI DSS requirements [1], is legal, and is enforceable.

1 Introduction

1.1 General

1.1.1 Scope

This site security policy applies to all information processed, stored, and transmitted on systems encompassed by the PCI DSS requirements [PCI 12.1.1]. The policies set forth in this document also apply to partner interfaces that connect to the Instant Systems networks and systems that are covered by the PCI DSS requirements. The systems encompassed by the PCI DSS requirements at Instant Systems include the systems in the Instant Systems Secure Zone (IS-SZ) described in [2], i.e., ID-DOCKER01, ID-DOCKER02, ID-DC01, ID-DC02, ID-EDR, ID-HV01, ID-HV02, ID-FRA, ID-MUST, ID-Polisen2, firewall and backups.

1.1.2 Purpose

The purpose of this document is to provide Instant Systems personnel and contractors with specific guidelines to follow with respect to information assurance and compliance with the PCI DSS requirements [PCI 12.1].

1.1.3 Compliance With This Policy

All personnel with access to IS-SZ must comply with this policy and acknowledge in writing that they have read and understood the policy [4]. The acknowledgement must be done at least annually [2]. Disciplinary actions may be taken for employees who do not comply with this site security policy [PCI 12.6.2]. Furthermore, references of applying personnel that are going to need access to the IS-SZ must be thoroughly examined to minimize the risk of attacks from internal sources [PCI 12.7].

1.1.4 Director of Information Security

The Director of Information Security (DIA) is responsible for maintaining and distributing this policy as well as establishing, documenting and distributing required security procedures [PCI 12.5] [PCI 12.5.1].

1.1.5 List of roles within Instant Systems

Kristian Silbvers, CEO
Pierre Larsson, VP
Sara Spånglund, CFO
Johan Snygg, CTO
Charles Carlsson, System Administrator – responsible for PCI compliance
Johan Gunnarsson Petersson, Software Development

1.1.6 Organizational Change Impact Review [12.5.3]

Significant changes to the organizational structure—such as mergers, acquisitions, or major internal restructuring—must trigger a documented internal review to assess the impact on the PCI DSS scope and the applicability of security controls. This review shall evaluate whether the current security measures remain effective and appropriate given the new structure. The results of this assessment must be formally documented and communicated to executive management to ensure continued alignment with PCI DSS compliance requirements

1.2 Security Awareness

A formal security awareness program to make employees with access to IS-SZ aware of the importance of cardholder data security must exist [4]. The program should rely on educating the personnel about this policy document both in written form and through meetings upon hire and at least annually [2]. Quarterly interviews of ID-SZ users should be done to confirm personnel are following security policies and operational procedures. In addition, a newsletter informing about security related issues should be distributed via email at least quarterly to all personnel encompassed by the security awareness program [PCI 12.6] [PCI 12.6.1] [PCI 12.11.1] [2].

1.3 Revision

Security procedures must be revised at least annually [2].

1.3.1 Annual Risk Assessment

Every manager must perform risk assessment of the company's security each year together with the CEO and DIA. The purpose is to identify potential threats and vulnerabilities in the system and must result in a formal risk assessment document. When the document has been produced, a project will be initiated to investigate how the company may protect itself from any threats identified [PCI 12.2].

1.3.2 Annual Revision

This policy will be revised as soon as the formal risk assessment has been concluded [PCI 12.1.1].

1.3.3 Environmental Changes

Environmental changes affecting the policy requires immediate revision of the policy [PCI 12.1.1]. Newly discovered security vulnerabilities must be identified and handled properly through subscription and regular monitoring of information sources (e.g., the "Fulldisclosure" and "Microsoft Focus" mailing lists via the site https://seclists.org/fulldisclosure/) [PCI 6.1]. Found vulnerabilities are ranked depending on potential impact [24]. See also [17] for security vulnerability monitoring at the hosting partner Splitvision. Testing must be performed after installing security updates to ensure that the vulnerability is no longer present.

2 Identification and Authentication

2.1 Unique ID

All computer systems included in the IS-SZ must incorporate access controls that employ a unique identification code (User ID) for each staff member or automated process with access to the IS-SZ. The following standards must be used across all platforms accessing IS-SZ:

* Each user of a system within the IS-SZ must have a unique identification code (User ID).

* The User ID credentials may never be handed over to another user, not even for a short period of time.

* Remote access to IS-SZ must be secured with two-factor authentication and must only be performed on company approved equipment [PCI 8.3.2].

* Remote access to IS-SZ must be performed using RDP across an encrypted VPN connection [PCI 2.3]. In particular, Telnet is NOT allowed to any of the systems in the IS-SZ.
* Unique ID username, password and client certificate and can't use a single factor without approved by management

* Can't use system/application accounts for interactive logins. [8.6.1]

* Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, files, source code or bespoke. [8.6.2]

2.2 Passwords

2.2.1 Length, Content, and Complexity

IS-SZ passwords are required to be at least 12 characters in length [PCI 8.3.6].
IS-SZ passwords must consist of a mixture of both numeric and alphabetic characters [PCI 8.3.6].
ID-SZ service or application accounts has to be 20 characters in length [PCI 8.6.3] and be renew every three years.

2.2.2 Expiration and Change

IS-SZ passwords as well as the passwords for the firewall must expire in 90 days and must be changed at the next login [PCI 8.3.9].

2.2.3 Password Etiquette

Employees must protect all IS-SZ system passwords, along with voicemail pin numbers, and email account passwords at all times. Individual IS-SZ passwords must NOT be shared with others. Users must NEVER access any IS-SZ computer system using another user's account or password. Users must be assigned a unique user id making them individually identifiable before allowing them access to the system components or cardholder data. [PCI 8.1.1]

2.2.4 Certificates

Assigned to specific people to keep in their computer which has to be protected by password and protection software, and they may not bring it somewhere else. [8.3.11]

2.2.5 Lost Authentication Factor "Passwords and VPN certificates"

In the event of lost or forgotten IS-SZ password, the affected user must verbally, and in person, request that the account password be reset to the default password. System administrators must verify a user's identification prior to resetting IS-SZ accounts and must NEVER act upon e-mail requests, or telephone requests, to reset a user IS-SZ account without proper verification of the user's identity [PCI 8.3.2].

2.2.6 User Responsibilities
Employees must maintain the confidentiality of their system passwords and must notify management upon a suspected IS-SZ password leak according to the procedures given in [2].

2.2.7 Creation of New Passwords
All initial passwords that are generated for new user login to IS-SZ must be unique. These passwords must also expire after the first use [PCI 8.3.5].

2.2.8 Password History
A password may not be the same as any of the last four used passwords. [PCI 8.3.7]

2.3 Eventlog Analyzer
At the login screen for the browser based tool Eventlog Analyzer, the "Keep me signed in"-checkbox shall not be checked.

2.4 Policy Enforcement
Users of Instant Systems' systems are expected to comply with this policy, independent of the operating system's ability to ensure compliance.

3 Account Management

In order to qualify for an account, all new users/employees must agree to a credit report lookup and supply criminal records directly from the police in an unopened envelope (to make sure it hasn't been tampered with). These two lookups are to ensure that new users doesn't have major debt or criminal tendencies.

3.1 Types of Accounts

3.1.1 User
User accounts are the primary and fundamental type of network accounts for all systems in the IS-SZ. Every user must have a unique User ID.

3.1.2 Administrator
Administrator accounts provide superuser, root access to servers and workstations. Administrator accounts are for system administrator job responsibilities, and must ONLY be used for administrative purposes in the IS-SZ. Every system administrator must have a unique administrator account [PCI 8.2.1]. Non-administrative duties are not allowed on the systems in IS-SZ.

3.1.3 Group
Group accounts are never allowed in the IS-SZ, even by special request. Each user must have a unique account [PCI 8.2.1].

3.1.4 Guest
Guest accounts are never allowed in the IS-SZ, even by special request. A normal user account must always be set up for a system in the IS-SZ, even if it is just for temporary access [PCI 8.2].

3.1.5 Default
Default accounts must be disabled on all systems in the IS-SZ [PCI 8.2].

3.2 Account Setup

Users must request new accounts to the IS-SZ in writing by sending an authorization form to the Operations group for approval by the Manager of Operations (OM). The approval is made by signing the authorization form. The Operations Group (see [12] for a list of members in said group) administrator then implements the approved user account according to the privileges specified in the authorization form. Instant Systems Sweden AB handles account for employees of Instant. [PCI 12.5.4]. The user shall be provided with an initial password that will be used to login to the IS-SZ the first time. The initial password must be unique and the user account must be configured in a way that requires the user change the password at the first login [PCI 8.3.5].
Every new user should be added in the Group, roles and responsibilities document.

3.3 Account Modification

IS-SZ account changes/modifications must be approved by the OM prior to being implemented by a system administrator [PCI 8.2.4]. The approval is made by signing the user's authorization form where the required changes/modifications are described.

3.4 Account Termination

Procedures must be in place to ensure that User IDs are removed from all systems in the IS-SZ when users are terminated, transferred, or no longer require access [8.1.3]. Account termination must be approved by the OM prior to being implemented by a system administrator [PCI 7.1.4]. The approval is made by signing the user's authorization form where the reason for termination is istated.

3.4.1 Terminated Users

User IDs must be removed from all systems in the IS-SZ immediately when the user is terminated [PCI 8.2.4].

3.4.2 Unused accounts

Every 90 days, a check must be performed on audit logs for successful login attempts to the IS-SZ in order to remove or disable any accounts not used for the last 90 days [PCI 8.2.6].

3.4.3 Vendor accounts

Accounts used by vendors to support and maintain any system component within the IS-SZ must only be enabled when needed by the vendor and monitored while being used [PCI 8.2.4].

3.5 Account Lockout

A user's login account must be automatically locked after six unsuccessful login attempts to the IS-SZ. The user must then contact the Support & Hosting Group to re-validate their account [PCI 8.3.4].

3.6 Authorizations

3.6.1 Account privilege permissions

By default, new accounts in the IS-SZ must be created with the fewest privileges available. Each manager is responsible for determining appropriate access requirements of every employee based upon their job responsibilities [PCI 7.1.2] and must sign an authorization form specifying the required privileges [PCI 7.1.3] [PCI 8.5.1]. Access control must be implemented via an automated system [PCI 7.1.4] and once a user has authenticated to the IS-SZ, they must have access ONLY to those network resources deemed appropriate to their job functions [PCI 7.1.1]. All multi-user system components in IS-SZ must be covered by the access control system [PCI 7.2.1] and assign privileges based upon job responsibilities [PCI 7.2.2]. The access control system should default to a "deny-all"

setting [PCI 7.2.3]. Administrator, super user and other root access privileges must only be granted to IS-SZ administrators with the need for such access within their job responsibilities, and must grant the least privilege required to perform the administration duties [PCI 7.1] [PCI 7.2].

3.6.2 Root Access, Super-User Privileges, and Local Administrative Rights

Users may be granted superuser or administrative rights to their workstations, personal computers or laptops. Administrative rights grant a user total control over their workstation. However, users are prohibited from de-installing pre-configured software (e.g. anti-virus scanner) and make any changes to the network configuration established by the Operations Department.

In addition, IS-SZ users are prohibited from installing any software that is not business related (i.e. games, screensavers) or other non-approved software or operating systems on any of the systems in the IS-SZ.

A server in the IS-SZ may be configured to allow IS-SZ users selected and justified local administration privileges when the requirement is properly documented by the OM and evaluated by the Operations Group. Regardless of the level of administrative access to any workstation, non IS-SZ users are expressly NOT permitted to the IS-SZ [PCI 7.1].

3.6.3 Executable Content

Only approved staff members are authorized to install or download any software on the systems in the IS-SZ.

3.6.4 Reactivation of idle sessions

If a session on the IS-SZ has been idle for more than 15 minutes, the user must re-enter the password to reactivate the session [PCI 8.1.8].

3.6.5 Revision

Users must be maintained in PCI - List of users [PCI 7.2.4] and be reviewed at least once every 6 months. Targeted Risk Analysis are to be completed during the same review. [7.2.5.1]

3.7 Acceptable Use

Internet and Intranet access, voice mail, electronic mail, and other communications systems are provided by Instant Systems to assist employees in obtaining work-related data and technology and effectively communicate work related information. The following guidelines have been established to help ensure responsible and productive Internet, Intranet and computer usage generally.

3.7.1 Expectation of Privacy

Recognizing the company's responsibility to protect employees’ personal privacy and dignity, Instant Systems must exercise great care and judgment in the collection, maintenance, use, and release of employee personal information. However, when using organizational computer assets, staff members should not expect any extraordinary privacy regarding their actions. All usage of computer systems must be in accordance with business policy and usage expectations.

Instant Systems-provided office furniture and personal computers are areas where the company's business information and employees’ personal property are likely to become commingled. For the majority of employees, and for most of the time, there is no problem with such commingling and management normally has no need to gain access to employees’ office furniture. On rare occasions, however, to obtain business information or for security reasons, it may be necessary for management to access an employee’s furniture and/or files, and it is important for employees to understand that Instant Systems has a legal right to do so. For these reasons, employees are cautioned not to keep sensitive

personal materials at the office, on their desktop computers, or on company file servers.

3.7.2 Personal Usage

Occasionally, employees may need to address personal matters during lunch or a break to make personal calls, e-mail personal messages, or perform Internet searches. On these limited and incidental occasions, Instant Systems understands the use of networks and systems for personal, non-business purposes, as long as the use is during non-work time, is not excessive, and does not include any of the prohibited uses under current policy. Employees are expected to demonstrate a sense of responsibility and to not abuse this privilege. Human Resources through managers remain the final authority within each work group regarding personal use of Instant Systems systems.

3.7.3 Prohibited System Usage

Data that is composed and transmitted through Instant Systems computer systems over the Internet or Intranet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to receivers or employees ('offending data'). Employees who receive offending data should notify the sender that the sender is not to transmit such data again, and that receipt of such data in the future will result in notification to the managers of Instant Systems. Examples of offending data may include, but are not limited to, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law. Content that is composed, transmitted or accessed, and is reasonably related to performing the employee's job responsibilities is not offending data under this policy, and therefore, is not prohibited to the extent it is needed to perform legitimate job responsibilities.
The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

* Sending or posting discriminatory, harassing, or threatening messages or images;
* Sending or posting confidential material, trade secrets or proprietary information outside of the organization;
* Attempting to break into the computer system of another organization or person;
* Engaging in any other illegal activities.

Employees must not use networks and systems in a manner that is likely to cause network congestion or significantly hamper the ability of other employees to access the system.

3.7.4 Misuse

Misuse of the company’s electronic communications systems is serious misconduct and may result in disciplinary actions. Employees subjected to inappropriate material through their computer or someone else's computer should contact their manager.

3.8 Accountability

Users are accountable for their actions when using the Instant Systems network. However, user accountability is predicated upon providing appropriate protections to user IDs, passwords, and pin codes. Employees are responsible for work performed under their passwords and/or access codes; therefore, employees must maintain the confidentiality of their system passwords. While passwords and codes used outside the IS-SZ may be shared in order to meet an appropriate temporary access business need, the password should be changed immediately thereafter. Anyone obtaining electronic access to another company's or individual's materials must respect all copyrights and cannot copy, retrieve, modify, or forward copyrighted materials, except as permitted by copyright owner.

4 Data Protection

4.1 Transmission of Sensitive Information

Reasonable care must be afforded to ensure that individuals who are not authorized are not provided access to sensitive information.

4.1.1 Electronic Transmission

Sensitive information sent over the Internet (by e-mail or any other means) should be encrypted prior to transmission with at least TLS 1.2 RSA 2048. In particular, credit card data may never be sent via end-user messaging technologies such as email, instant messaging or chat [PCI 4.2] [PCI 12.3]. It is also important that sensitive e-mail or documents stored with online services such as Office365 and Sharepoint Documents are accessed using encrypted connections, e.g., SSL (https).

4.1.2 Certificate

The certificate used for web access on the web server must be issued by a Trusted Authority.

4.1.3 Facsimile

If sensitive information is sent via fax, the receiving party's fax number should be confirmed and should be notified of the transmission just before the fax is sent so that the fax machine receiving the fax is attended to.

Credit card data may never be sent via fax [PCI 9.7].

4.1.4 Courier

If sensitive information is sent via courier, the sender should confirm the receiver's address and alert the receiver of the package's departure and the courier company's prescribed latest delivery time. Further, a copy of the waybill should be retained so that the package may be tracked in the situation where the package does not arrive on time [PCI 9.6.2].

4.1.5 Post

If sensitive information is sent via regular mail, the sender should confirm the receiver's address and alert the receiver of the package's departure. Credit card data may never be sent in paper format via regular mail [PCI 9.6.2].

4.1.6 Employee-facing Technologies

Only employ company approved employee-facing products are allowed for accessing credit card data [PCI 12.3.7] and must be listed in [11].

Credit card data may occasionally be accessed through remote access equipment using two-factor authentication (see ISP 2-1) [PCI 12.3.2]. The technology employed for remote access has to be explicitly approved by authorized parties [PCI 12.3.1] and a list of all devices and personnel with access to use the devices must exist [PCI 12.3.3]. Each device must be labelled with owner, contact information and purpose [PCI 12.3.4]. Remote access sessions must be automatically disconnected after 30 minutes of inactivity [PCI 12.3.8] and may only be activated for vendors and business partners when needed (thus, immediately deactivated after use) [PCI 12.3.9]. Credit card data obtained through remote access methods must not be stored on local hard drives or removable media [PCI 12.3.10]. Using remote access equipment for accessing credit card data is only acceptable for software development, testing, debugging and when required by the daily operational security procedures in [2] [PCI 12.3.5]. Credit card data may only be remotely accessed from company approved network locations [PCI 12.3.6]. The network locations approved by Instant Systems include most common network locations such as the offices of Instant Systems or its partners, homes of the employees, or hotels, as long as the credit card data

is accessed through computer equipment approved by the company.

Removable media, laptops and personal digital assistants are generally not allowed inside the IS-SZ. However, should these devices be required for accessing credit card data, the rules for remote-access devices described above must apply also in this case [PCI 12.3]. USB-sticks is only allowed if it is verified by PCI Admins and if it is needed for maintenance of PCI equipment.

Credit card data may never be accessed by modems and wireless. This applies to employees as well as contractors [PCI 2.1.1], [PCI 4.1.1] [PCI 12.3].

4.2 Proprietary Data Away from Instant Systems Control

Reasonable care must be afforded to ensure that sensitive data taken outside of Instant Systems spaces is protected. Thus, all sensitive information recorded on portable media (magnetic tapes, floppy disks, optical disks, etc.) that is taken off-site should be marked as "confidential", encrypted, logged and must never be taken outside of Instant Systems without proper authorization by management [PCI 9.7] [9.7.1], see also [17] for a description of the hosting provider commitments [PCI 9.9] [PCI 2.4].

4.3 Laptop Computers

Reasonable care must be taken when laptop/mobile devices is connecting to PCI environment because of vulnerable to exploitation if the laptop/mobile device is lost or stolen. Laptops/mobile devices that has connected to PCI environment should never be taken outside of Instant Systems spaces and should be disk encrypted. For best practise, only stationary computers should ever be connected to PCI zone.

4.4 Internal Very Sensitive Information

Although measures are in place to protect critical Instant Systems information from disclosure to outside parties, certain types of data are extremely sensitive, and must be tightly protected within Instant Systems controlled areas as well. This information include credit card data and passwords for all IS-SZ systems. All information in these categories must be rendered unreadable using industry standard strong cryptography in transmission, and remain encrypted in storage. E.g., standard FTP which uses plain text transmission of passwords is not allowed to any server in the IS-SZ. See [3] for a detailed description of credit card data protection procedures at Instant Systems [PCI 3.2] [PCI 3.3] [PCI 3.4] [PCI 3.5] [PCI 3.6] [PCI 4.1] [PCI 8.4].

4.4.1 Monitoring of Credit Card Data

The DIA must ensure that all accesses to credit card data are monitored and controlled [PCI 12.5.5].

4.4.2 Sharing of Credit Card Data

If cardholder data is shared with service providers, then contractually, service providers must adhere to the PCI DSS requirements [PCI 12.8.1] and acknowledge that they are responsible for the security of cardholder data the provider possesses [PCI 12.8.2].
Media containing credit card data that is moved from IS-SZ must be logged and approved by management [17] [PCI 9.8].

4.4.3 Destruction of Credit Card Data

Credit card data must be securely destroyed after it is no longer needed. This includes credit card data in the server environment [PCI 3.2] [PCI 9.8].
The following methods must be followed:

* Paper copies - must be cross-cut shredded [PCI 9.8.1].
* Electronic copies on internal servers - must be deleted.

* Electronic copies on removable media - must be securely wiped from the storage media using a method that overwrites every bit in the file, see also [17] [PCI 9.8.2].

4.5 Need-to-Know

Prior to disclosing proprietary information, all employees must ensure that he or she is authorized to disclose such information and that the recipient is authorized to receive the information. If the recipient is an employee of Instant Systems, it is the disclosing employee's responsibility to ensure the recipient is authorized or requires access to such information in order to perform his Company-assigned responsibilities.

5 Auditing

5.1 Parties Responsible for Audit and Audit Review

The DIA must specify the audit method and frequency and ensure that security alerts and information is distributed to appropriate personnel [PCI 12.5.2]. The SLA department is responsible for monitoring security alerts and distributing information to the Instant Systems Operations Group for further analysis and handling.

5.1.1 Audit Review Schedule and Reporting

Automated audit log reviews must take place in semi-real time through a continuously running automatic analyzer tool (e.g., Event Log Analyzer [2][7]). Since correct time-stamping is important, all critical system clocks and times on IS-SZ have to be synchronized through a common NTP-server which uses a public internet server for its time synchronization. Configure according to [2][PCI 10.4].

The results of all system and application audits must be automatically analyzed and reports created. If suspect activity is detected a high priority alert must be sent 24/7 [PCI 10.6] by personnel at the hosting partner Splitvision to be handled by the Instant Systems Operations Group.

CTO has to

5.2 Audit Logs

5.2.1 Contents

All access to system components must be linked to each individual user (e.g., by running the report "Track Individual User Action report" in Event Log Analyzer) [PCI 10.1] [PCI 10.2.2].

All individual user access to cardholder data must be tracked (e.g., through the "User Logon report" and "User Logoff report" combined with logs obtained from the database server) [PCI 10.2.1].

All users who have reviewed audit trails must be tracked (e.g., through "Track Audit Policy Changes report") [PCI 10.2.3].

All failed login attempts must be tracked (e.g., through the "Logon Failure report") [PCI 10.2.4].

Identification and authorization must be tracked (e.g., by using the "User Logon report" and "Logon Failure report" together with logs from the database server showing the actual database logins) [PCI 10.2.5].

Initialization and access of audit logs must be tracked (e.g., through the "Audit Logs Access report") [PCI 10.2.6].

Changes of system-level objects must be tracked (e.g., through the "Object Access report") [PCI 10.2.7].

The EventLog Analyzer records user identification, type of event, date and time, success or failure indication, origination of event and identity of name of affected data, system component or resource [PCI 10.3].

5.2.2 Safeguards

To review audit logs, the user must be logged onto the VPN to the IS-SZ and have a user account to the Event Log Analyzer. Only users that need to review audit logs may obtain such an account [PCI 10.5.1]. Audit logs must be protected from unauthorized modifications [PCI 10.5.2] and backuped immediately [PCI 10.5.3] [2].

The file integrity system described in [2] must also be used for monitoring and detecting changes on logs [PCI 10.5.5].

No wireless networks are allowed in IS-SZ (if such networks would be employed, the logs from these must be copied to the log server on the internal LAN [PCI 10.5.4]).

5.2.3 Retention

Audit logs containing security relevant events must be retained according to [8] [PCI 10.7]. During the retention period, audit logs must be secured such that they cannot be modified, and such that only authorized persons can read them.

5.3 Security Incidents

5.3.1 General

When security incidents occur, such as possible criminal activity or disciplinary action, the CEO, DIA, Manager of Operations, Manager of Software Development and the hosting partner must be informed. The hosting partner must if instructed remove the Internet connection to ID-DOCKER01 and ID-DOCKER02 immediately and an ad-hoc audit board must convene to audit the affected systems. All reports from the ad-hoc board must be forwarded to the DIA who is formally responsible for updating the Incident Response Plan [PCI 12.5.3]. ID-DOCKER01 and ID-DOCKER02 may be reconnected to the Internet when the CEO, DIA, Manager of Operations and Manager of Application Development concludes that potential threats no longer exist. If an external intrusion has occurred, this has to be reported to the police.

5.3.2 Incident Response Plan

When security incidents occur, employers and contractors are required to follow the Instant Systems Incident Response Plan [PCI 12.9.1] given in [2].

5.3.3 Jour

We maintain a 24/7 incident response readiness through all members of the management team. This team is responsible for receiving alerts regarding suspected or confirmed security incidents and initiating appropriate response actions. [12.10.3]

Alerts are received via multiple channels—email, text messages, and phone calls—to ensure prompt awareness regardless of time or location. Upon receiving an alert, the management team member on duty or available takes immediate action by contacting the appropriate personnel or team based on the nature and severity of the incident.

This approach ensures that trained and authorized individuals are always available to initiate a timely response, minimizing potential disruption and ensuring alignment with our incident response procedures.

5.3.4 Monitoring
Automatic systems for detecting security incidents in the IS-SZ should include file integrity monitoring systems (e.g. Manage Engine FIM [10]) as well as intrusion prevention and detection systems (e.g. SNORT [9]) [PCI 12.9.5]. In addition, automated audit log reviews must be conducted regularly, see 5-1-1.

5.3.5 Personnel Availability
Specific personnel must be available on a 24/7 basis to respond to alerts, especially evidence of unauthorized activity, critical IDS alerts or reports of unauthorized critical system or content file changes must be responded to [PCI 12.9.3].

5.3.6 Training
Staff with security breach response responsibilities must be adequately trained as a part of the security awareness program described in 1-2 [PCI 12.9.4].

5.3.7 Test
To ensure that security incidents will be handled properly, the Instant Systems Incident Response Plan must be tested annually [PCI 12.9.2] according to the test procedure given in [2].

5.3.8 Revision
All security incidents must be documented and the incident response plan must be modified according to lessons learned. Industry developments must be incorporated into the incident response plan as soon as they are effective [PCI 12.9.6].

6 Malicious Code and Anti-Virus Scanning

The term "Malicious Code" is a catch all term that refers to many types of computer software that cause harm to a computer system. Not all malicious code is necessarily intended to cause harm. The harm may be a side-effect of the code, or the harm may simply be that the code is running on a system without proper authorization.

6.1 Anti-Virus Software

Antivirus software must be deployed and remain up-to-date on all systems commonly affected by viruses [PCI 5.2]. Furthermore, in addition to malicious code, the anti-virus software must protect against both adware and spyware [PCI 5.1]. Full logging must also be enabled in the anti-virus software and the logs retained online for at least three months while archived logs must be available for at least one year [8] [2].
It is required to do a risk analysis malware every 6 months.[5.3.2.1]

Antivirus ska konfigureras så att det uppdateras automatiskt och genomför periodiska genomsökningar. Loggar ska sparas minst minst 3 månader online, minst 1 år totalt [Malware 7].

6.2 Corporate Workstations

Every corporate workstation and mobile workstation must employ anti-virus software.

6.2.1 Signature Updates
The anti-virus software must be configured to seek a signature update from the vendor at least every seven days [2]. Additionally, users must not modify or disable the virus signature update schedule for the virus scanning application [PCI 5.2].

6.2.2 Scan Frequency
Antivirus software must be running as a background process at all times.

6.2.3 Scan Disable
Users are prohibited from disabling the virus scanning application on corporate workstations.

6.3 Servers
All servers must employ anti-virus software.

6.3.1 Signature Updates
The anti-virus software must be configured to seek a signature update from the vendor at least every seven days [PCI 5.2] [2].

6.3.2 Scan Frequency
Antivirus software must be running as a background process at all times. Additionally, the virus detection software must perform a full system scan on a daily basis.

6.3.3 Email Attachments
The virus detection software must check every email attachment before allowing the server to forward the message to its final destination. If a virus is encountered, the systems administrator must be notified immediately and the offending message must not be forwarded to its final destination.

6.4 Mobile Workstations
All mobile workstations, laptops and portable computers must employ anti-virus software.

6.4.1 Signature Updates
The anti-virus software must be configured to seek a signature update from the vendor at least every seven days [2]. Additionally, users must not modify or disable the virus signature update schedule for the virus scanning application [PCI 5.2].

6.4.2 Scan Frequency
Antivirus software must be running as a background process at all times.

6.4.3 Scan Disable
Users are prohibited from disabling the virus scanning application on mobile workstations, laptops and portable computers.

6.5 Virus Notification Process
Employees are required to notify the DIA immediately upon receipt of a suspected computer virus.

6.5.6 Vulnerability Monitoring Process
SLA is required to monitor Fulldisclosure, Pfsense, Microsoft buglist for new vulnerabilities that can harm or enable unallowed access to PCI servers and network to unauthorized users. Review of these sources should be done on monthly basis and discovered problems should be fixed as soon as they are detected. New security problems should be documented in Vulnerability listing and ranking document and scored based on CVSS.

7 System Configuration Management

7.1 Configuration Control

All computer and communications systems used for credit card processing are considered critical systems. Accordingly, they must employ a formal change control procedure [2] authored by the Maintenance & Hosting Group. All servers in IS-SZ must be configured according to the Instant Systems server configuration standard described in [7] [PCI 2.2] [PCI 2.2.3]. In particular, only one primary function should be implemented per server [PCI 2.2.1] and all unnecessary functionality, services and protocols must be removed [PCI 2.2.4] [PCI 2.2.5].

7.1.1 Change Control Process

Prior to being installed, new or different versions of the operating system and related systems software for IS-SZ systems must go through the established change control process [2] [PCI 6.4]. Executable software application modules, including both internal and external web application modules, must be developed according to the Instant Systems Development policy given in [2] [PCI 6.3] [PCI 6.5]. Consequently, they must never be moved directly from test libraries to production libraries. Fully tested modules must be reviewed and then re-compiled before being moved to production libraries. This process is designed to help detect and eradicate errors as well as Trojan Horses and other unauthorized code. The formal written change control process must be used to ensure that all business application hardware and software moves into production only after receiving proper authorization.

7.1.2 Regular Updates

All software and firmware running on the servers and network units in IS-SZ must be checked for updates and updated at least every 30 days [PCI 6.1] [2]. Instant Systems, SLA, is responsible for updating networking components as well as software components.

7.2 Software Licenses

Unlicensed (pirated) copies of commercial software are expressly forbidden. Only software licensed to Instant Systems may be installed on any computing system in IS-SZ.

8 Backups

8.1 Information Requiring Backup

All critical business information resident on IS-SZ computer systems must be subjected to back-up.

8.2 Backup Schedule

The backup processes must be performed with sufficient frequency to support documented contingency plans. Thus, the on-duty administrator must perform backups for all files in the IS-SZ each business day.

8.3 Backup Storage

8.3.1 Fireproof, Locked Cabinet

Backup media stored locally must be secured in a fireproof, locked cabinet in a restricted area which is visited periodically to ensure that these security conditions are met [17] [PCI 9.5].

8.4 Retention Period

The data retention requirements are described in [8] [PCI 3.1].

8.5 Backup Integrity

8.5.1 Testing: Backups and Media

The computer data media used for storing proprietary information must be high quality and must be periodically tested to ensure that it can properly record the information in question. Used data media that can no longer reliably retain information must not be used for archival storage. Proprietary business information and software archived on computer storage media for a prolonged period of time must be tested regularly to ensure that the information is still recoverable.

9 Physical Security

9.1 Access to Key Facilities

Access to the equipment and facilities of the IS-SZ is restricted and governed by the hosting partner procedures [17] [PCI 9.1] [PCI 9.2] [PCI 9.3] [PCI 9.4] [PCI 9.6].

Employed personnel shall carry license cards with a photo of themselves.

All authorization cards must be handled with very restrictive access by Splitvision, passages to the datacenter are logged for 14 days. Normally, the system is managed by an administrator only. Backup for sickness vacation shall be available. All changes regarding authorization cards must be logged in the passport database. [PCI 9.2b]

All lost cards shall be locked immediately by short-circuit function. Personnel who terminate their employment shall return their license card. [PCI 9.2a]

All visitors who do not have a license card must be verified by PCI Authorized personnel at Instant Systems AB. [PCI 9.3.1] [PCI 9.3.2]

Visitors have to be monitored during the entire visit by PCI Authorized personnel. [PCI 9.3.3]

Instant Systems enforce camera surveillance 24/7 in their headquarters.

9.2 Instant System Backups to Hard Drive

Credit card information must be secured physically. If credit card details end up on paper, the paper must be destroyed. If credit card details end up on electronic media, they must be removed with a military grade wipe program or physically destroyed. Disabled server hard drives or backup tapes should be physically destroyed. If temporary storage of media is used before destruction occurs, the storage should be secure. All media must be logged [13]. [PCI 9.6]

All stored information and media such as tape cartridges handled within Splitvision Production are classified as confidential and should therefore be handled accordingly. [PCI 9.7.1]

Information and media sent from us are handled in accordance with the agreement with the relevant customer. Media sent for remote control is logged and handled by self-employed personnel. All media sent outside the facility should be logged and authorized by management and sent via secured courier or other delivery mechanism that can be tracked. [PCI 9.7.2]

All media of any type that contain credit card details and moved from secured zone must be logged [13] and authorized by management. [PCI 9.8]

10 Daily Procedures

10.1 Daily Operational Security Procedures

Daily operational security procedures must be in place which are consistent with the PCI requirements [PCI 12.2], i.e. the procedures given in [PCI 1] [PCI 3] [PCI 6] [PCI 8] [PCI 11] [PCI 12]. A detailed description of the daily operational security procedures affecting Instant Systems and hosting partner is given in [2].

11 External (Network) Connectivity

11.1 Intrusion Detection Systems

All Internet-connected networks in the IS-SZ must use an intrusion detection system approved by the DIA (e.g., SNORT Intrusion Detection [19]). Network Security Administrators must respond to suspected network intrusions according to the PCI Incident Response Plan [2] [PCI 11.4].

11.1.1 Signature Updates on a Regular Schedule

All IDS component attack signature databases must be updated at least every 30 days [PCI 11.4] [2].

11.2 Connections to Partners

* All network connections between the IS-SZ and trusted partners (entities) must undergo risk assessment prior to activating the connection [PCI 12.10.2].
* The risk assessment must include procedures for ensuring that the entity is PCI DSS compliant [12.10.3].
* A list of entities connected to the IS-SZ must be maintained [5] [PCI 12.10.1].
* Connecting and disconnecting entities must follow the procedure described in [2] [PCI 12.10.4].

12 References

[1] Payment card industry (pci) security standard

[2] Instant Systems Policies and Procedures

[3] PCI Protection of stored credit card information

[4] PCI Formellt säkerhetsmedvetenhetsprogram

[5] PCI List of Connected Entities

[6] PCI Instant Systems Services, ports and protocols

[7] http://manageengine.adventnet.com/products/eventlog/

[8] http://www.aqtronix.com/?PageID=99

[9] http://www.snort.org

[10] https://www.newnettechnologies.com/change-tracker-gen-7.html

[11] PCI Nycklar och kort

[12] Authorization Form data for Instant Systems Secure Zone Users

[13] PCI Media Inventory Log