Joint-Stock Company
«Common Republican
Processing Center»

Appendix No. 2
to the Rules of the «UZCARD»
Payment System

STANDARD OF UZCARD PAYMENT SYSTEM

Requirements of information security of Payment system «UZCARD»

(Version 3.1)

Tashkent – 2025

1. TERMS AND DEFINITIONS

For the purposes of the Standard, terms and definitions are used in the meanings established by the Law of the Republic of Uzbekistan dated 01.11.2019 №ZRU-578 " About payments and payment systems", the Law of the Republic of Uzbekistan dated 05.11.2019 №ZRU-580 "About banks and banking activities", regulatory documents of the Central Bank of the Republic of Uzbekistan, Rules of Payment system "UZCARD", as well as other acts of legislation of the Republic of Uzbekistan.
In the Standard, unless the context otherwise requires, words used in the singular may also imply the plural and vice versa, and words used in the masculine gender may also imply the feminine and neuter gender and vice versa.

2. GENERAL PROVISIONS.

2.1 This Standard is a document that establishes the procedure and terms of interaction between ICTV Subjects when receiving the IP Service on BC, as well as other terms of information and technological interaction.
2.2 This Standard is designed to organize the information exchange necessary to ensure the operation of the IP Service.
2.3 Procedure for ICTI Subjects to adhere to this Standard:
- Participant of PS "UZCARD" - based on a valid contract with URPC for service in the processing center and in the presence of a valid contract with URPC for provision of automated data processing services through API of software "SV-Gate";
- Software - by acceptance of the Offer on interaction with PS "UZCARD" and in case there is a valid Agreement with URPC for provision of automated data processing services through API of "SV-Gate" software.
2.4. Adherence to this Standard means acceptance by ICTI Subjects of all terms and conditions of this Standard, Rules of PS "UZCARD" without any exceptions or limitations.
2.5. This Standard outline information security requirements for Partners to enable their connection and operation with the PS "UZCARD" and the SV-Gate software, which serves as a unified payment gateway for processing online transactions with bank cards.
2.6. Normative-Legal Acts and Standards Used in the Development of this Document:

• Law of the Republic of Uzbekistan "About Payments and Payment Systems" No. ZRU-578, dated November 1, 2019;

• Law of the Republic of Uzbekistan No. ZRU-547 "About Personal Data," dated July 2, 2019;

• Payment Card Industry Data Security Standard "PCI DSS Requirements and Testing Procedures" 4.0. 2.7. This Standard establishes requirements for Partners to ensure a baseline level of information security for payment

instruments that store, process, and transmit bank card data obtained through the unified payment gateway “SV-Gate.” Additionally, the document provides recommendations for improving Partners’ information security systems to achieve a higher level of information security.
2.8. Information security requirements applied to Partners during technical audits are specified in Appendix 1 of this Standard.

Appendix 1
To STANDARD OF PAYMENT SYSTEM UZCARD

Requirements of information security of Payment system "UZCARD"

№	Requirements	Verification Procedures
1	SECURITY DOCUMENTATION Implement and maintain normative-regulatory documents on information security.	
1.1.	Develop, publish, maintain, and disseminate an up-to-date information security policy. 1.1.1. Review the information security policy at least once a year and update it in case of changes in the Partner's environment. 1.1.2. Maintain a log of acknowledgment of the Information Security Policy and ensure it remains up-to-date.	Verify the current version of the information security policy. Review the policy change log to confirm the existence of a review cycle. Check the acknowledgment log for the information security policy and ensure that all employees interacting with the information security environment have been familiarized with it.
1.2.	The information security policy must be supported by local normative documents to facilitate the management and implementation of information security protection measures at the Partner's organization. These local normative documents must comply with the requirements of the Information Security Policy and supplement it in managing specific domains of information security protection measures. Examples of such local normative documents may include: -Regulations for ensuring antivirus protection (protection of systems from malicious software) -Regulations for software development and testing -Policy on authentication and account password management -Policy on the registration and monitoring of information security events.	Verify the document registry to confirm the presence of local normative documents supporting the information security policy. Second-level documents may also be specified in the main Information Security Policy as separate appendices to the policy.

1.3.	Implement a risk assessment process that is conducted at least once a year and following significant changes in the Partner's environment structure, identifies critical assets, threats, and vulnerabilities, and concludes with a formally documented risk analysis.	Verify the existence of an up-to-date document outlining proper risk assessment processes.
1.4.	Introduce a formal information security awareness program for the Partner's employees, the purpose of which is to inform the Company's employees about security policies and procedures. 1.4.1 Provide training to Partner's employees upon employment and at least once a year. 1.4.2 Require the Partner's personnel to confirm their knowledge and understanding of the Partner's information security policies and procedures at least once a year.	Verify the existence of this clause in the IS Policy or other documents, obtain up-to-date data on ISP training of the Partner's employees. At least the responsible employees interacting with the audited ISP environment should be trained. Verify whether the Partner's employees have passed annual IS knowledge tests.

1.5.	Develop an incident response plan applicable in the event of a system breach. Be prepared to respond immediately to an information system breach. 1.5.1 Analyze and test the incident response plan at least annually. 1.5.2 Include in the plan procedures for responding to alerts from information security monitoring systems, including, without limitation, intrusion detection and prevention systems, firewalls, and file integrity monitoring systems.	Request an incident response plan and ensure that the plan is up to date, reviewed and tested regularly.

1.6.	Ensure that security policies and firewall management operating procedures are documented, used and known by all involved Partner employees.	Verify that an up-to-date firewall management document is available.
1.7.	Develop configuration standards for all system components of the ISP environment. Ensure that the standards address all known security vulnerabilities as well as the provisions of generally accepted industry standards for secure configuration. Examples of sources of generally accepted industry standards for secure configuration include: - Internet Security Centre (CIS Benchmark); - International Organization for Standardization (ISO); - Institute for Systems Administration, Audit, Networking, and Security (SANS); - National Institute of Standards and Technology (NIST).	Selectively verify approved current configuration standards

1.8.	Implement user identity management procedures on all system components of the ISP environment governing the following requirements: - Immediately revoke access from accounts of terminated Partner employees. - Delete/block inactive accounts at least once every 90 calendar days - Limit access attempts by locking out a user ID after six consecutive unsuccessful account login attempts. - Set the account lockout time to 30 minutes, or until an administrator lifts the lockout. - If a user session is idle for more than 15 minutes, require users to re-authenticate to resume the terminal or session.	Verify that user identity management procedures are in place.
2	PHYSICAL SECURITY Ensure physical security of the segment of the ISP that receives, processes and stores payment card data. Limit physical access to the ISP environment.	
2.1.	Use proper room access controls to restrict and monitor physical access to systems in the ISP environment. 2.1.1 Use a video surveillance system (VSS) to control physical access to a critical room in the ISP environment. 2.1.2. Use an access control and management (ACM) system or mechanisms to control physical access to a critical room in the ISP environment. 2.1.3 Analyze data collected by access control systems and mechanisms. Store such data for at least three months. 2.1.4 Restrict access to wireless access points, gateways, portable devices, network communication equipment and communication channels.	In case the ISP server infrastructure is located in a Partner's building where the Partner is directly responsible for physical protection, verify the use of access control facilities in the premises (Data Centre). In case the ISP server infrastructure was leased from a service provider on the basis of a contract (virtual machine environment, colocation), check whether there is an appropriate clause in the contract on the responsibility for the physical protection of the equipment by the service provider.

2.2.	Develop procedures to easily distinguish between Partner employees who have access to the ISP environment to include: - Identifying Partner employees. - Modification of access rights. - Procedures for revoking or disabling the means of identification of terminated Partner employees. Ensuring that security policies and procedures for restricting physical access to the ISP segment are approved by management, utilized and known to all interested Partner employees.	Request a list of the Partner's responsible employees who have access to the server room.
2.3.	Control employee physical access to critical areas as follows: - Access must be authorized based on job responsibilities - Partner employee's access is instantly revoked upon termination and all physical access devices (e.g., keys, access cards, biometrics, etc.) are returned and disabled by them.	Request applications for access to the server room.
3	NETWORKSECURITY Install and maintain firewall configuration to protect data in the ISP environment.	
3.1.	Develop and implement firewall and router configuration standards 3.1.1. Develop a formal process for approving and testing all network connections and changes to firewall and router configurations.	Ensure that an up-to-date network design and data flow diagram of the payment cards of the ISP segment has been implemented. Study the current network design and data flow diagram of UZCARD payment cards.

	3.1.2 Implement an up-to-date network diagram showing all connections to the ISP environment from other networks, including all wireless networks. 3.1.3 Implement an up-to-date schema showing all payment card data flows in the ISP environment derived from SV-GATE software across systems and networks.	Verify that a formal process has been established to approve and test all network connections and changes to DOE configurations.

3.2.	Restrict incoming and outgoing traffic to connections required for the COI environment, deny all other traffic. 3.2.1 Configure connection restrictions on firewalls and routers between other networks and any system components in the ISP environment. 3.2.2 Review firewall and router rule sets at least semi-annually.	Check the firewall rules for default and any-any rules. Ensure that connection restrictions have been configured in the ISP environment. Ensure that firewall and router rule sets are reviewed at least semi-annually.
3.3.	Prohibit direct public access between the Internet and any system components in the ISP environment. 3.3.1 Implement a demilitarized zone (DMZ) to restrict incoming traffic to only those system components that provide authorized access to publicly available services, protocols and ports. 3.3.2 Restrict incoming Internet connections to addresses within the DMZ. 3.3.3 Prohibit unauthorized outbound traffic from the COI environment to the Internet. 3.3.4 Place system components (e.g., databases) that store cardholder data on an internal network segment separate from the DMZ and other untrusted networks.	Make sure that the ISP's main system components do not have direct access to the Internet, nor do the ISP's main system components have direct access to the Internet. Check that the Internet connection in the ISP segment is via the DMZ. Ensure that the system components that store card data are located on an internal network segment separate from the DMZ.

	3.3.5 Do not disclose private IP addresses and routing data to third parties who do not have authorized access to such information. Note: IP addressing concealment techniques include, but are not limited to: - Network Address Translation (NAT) technology; - placing servers containing cardholder data behind proxy servers/firewalls.	

3.4.	Use intrusion detection and/or prevention mechanisms to detect and/or prevent intrusion into the network. 3.4.1 Monitor network traffic at the perimeter of the ISP environment and at critical points within the ISP environment, and notify Partner's employees of suspicious activities. 3.4.2 Maintain intrusion detection and prevention systems and their signatures up to date.	Check the firewall settings to ensure that the network intrusion detection and/or prevention modules are enabled. These mechanisms can also be deployed separately from the primary firewall.
3.5.	Control and monitor any access to network resources. 3.5.1 Implement an event log linking any access to system components to a specific user.3.5.2 Configure event logs to send events to a centralized event acquisition system (SIEM).	Check events from the centralised event collection system for firewall ingress/egress events. Verify that the event log is implemented. Verify that the Event Log is configured to send events to the SIEM. Verify the implementation of the event log. Verify that the Event Log is configured to send events to the SIEM.

4	SECURITY OF SERVERS AND SYSTEM COMPONENTS Ensure the security of servers and system components of the ISP environment	
4.1.	Configure all system components of the ISP environment based on formally approved configuration standards. 4.1.1 Do not use default passwords and other system security parameters set by the manufacturer 4.1.2 Enable only necessary services, protocols, daemons, etc. required for system operation.	Selectively check the ISP system components for updated security settings. Verify that the system settings are not default and have been configured according to an approved configuration standard.
4.2.	Use strong cryptographic algorithms to encrypt the channel when using non-console administrative access to the system.	Check remote access settings to ISP servers, such as SSH settings and ensure that strong encryption methods are used for remote access to ISP servers.

4.3.	Maintain a log of system components that fall within the scope of the technical inspection.	Check the presence of this logbook. The system component log can be a document with a table of all system components of the ISP environment.
4.4.	Protect all systems from malware and regularly update antivirus software or programs - Deploy anti-virus software on all systems exposed to malware (especially workstations and servers). - Ensure that anti-virus software is capable of detecting and removing all known types of malwares, and providing protection against all known types of malwares.	Check the current anti-virus software license and the date of the last update in the sampled device.

	Guarantee that all anti-virus mechanisms: - Keep up-to-date. - Perform periodic scans. - The file protection module is enabled - - Create event logs and forward events to a centralised event collection system.	

4.5.	Develop and maintain secure systems and software 4.5.1 Implement a process for identifying vulnerabilities using authoritative external sources of vulnerability information, and managing the risk (e.g., 'high,' 'medium,' or 'low') of newly discovered vulnerabilities. 4.5.2 Ensure that all system and software components are protected against known vulnerabilities by installing vendor-issued security patches. Install critical security patches within one month of their release date. Note. Which security patches are considered critical should be determined based on a risk analysis? 4.5.3 Delete developer accounts, test and/or user accounts, user IDs and passwords before applications are put into production mode or made available to clients.	Check application servers selectively for update history and security patch installation history. Verify that security patches are installed and that critical patches are installed in a timely manner. Request an up-to-date report on the work performed to identify and remediate vulnerabilities by installing security patches. Ensure that a process has been established to identify vulnerabilities through authoritative external sources.

4.6.	Check written program code (automatically or manually) for potential vulnerabilities before it is put into production mode or made available to customers and ensure that: - Changes to the code are reviewed by other employees who are not the authors of the code, as well as by employees familiar with code review techniques and secure programing principles. - The code is developed in accordance with safe programming principles. - Necessary adjustments are made prior to software release. - Results of code review are reviewed and agreed with management prior to software release. Note. This code review requirement applies to all written code (both internal and public systems) within the system development lifecycle. Code reviews may be performed by competent internal personnel or by third parties. 4.6.1 Adhere to system component change management processes and procedures. 4.6.2 Prevent common software code vulnerabilities during the software development process as follows: - Train developers at least annually on current secure programming practices, including training on how to avoid common software vulnerabilities.	Obtain information on what work is being done to test the software code and work on identified vulnerabilities in the code and in the libraries used. Ensure that system component change management processes and procedures are followed. Note. The latest version of such requirements should be used, e.g. OWASP, SANS CWE Top 25, CERT Secure Coding, etc.

	- Develop applications according to the basic principles of secure programming. Note. The current version of such requirements should be used, e.g., OWASP, SANS CWE Top 25, CERT Secure Coding, etc. 4.6.3 Study new threats and vulnerabilities to publicly available web applications on an ongoing basis and ensure that these applications are protected from known attacks using the following methods: - Checking publicly available web applications for vulnerabilities using methods, manual or automated security analysis tools at least annually and after any changes are made. - Installing a technical tool in front of publicly accessible web applications to continuously inspect all traffic (e.g., an application layer firewall) to detect and prevent web-based attacks.	
4.7.	Separate development/testing environments from production environments, and implement access differentiation mechanisms.	Check that there are separate segments for production and test environments. Make sure that there is no access between segments.
4.8.	Divide responsibilities between employees with development/testing duties and those in the production environment.	Ensure that employees working in the test environment do not have access to the production environment. Work with the production environment may only be carried out by individual responsible employees appointed by order or other supporting document.

4.9.	Do not use production data (valid cardholder master numbers) for testing and development.	Request a selection (select) from the test environment database with the availability of payment card data and check its reality and relevance.
4.10.	Delete all test data and accounts from the system before putting such system into operation / production mode.	Interview Partner personnel on the method of translating the test environment into a production environment. Check the production environment for missing test data.
4.11.	Synchronize all system clocks and system time on critical systems and ensure that the following requirements are met for obtaining, distributing and storing time data: - Set accurate and consistent time on critical systems. - Obtain time settings from industry recognized sources.	Request data on the availability of a centralized system for synchronizing the system clock. Verify that the ISP servers are configured to synchronize the system clock.
5	SECURITY OF PAYMENT CARDS DATA DURING THEIR STORAGE AND PROCESSING. 5. Ensure protection of payment card data received from SV-Gate software during their storage and processing in database management systems (DBMS)	
5.1.	Limit data storage to the bare minimum necessary.	Request information about the purposes and processes for which "UZCARD" payment card data is used.
5.2.	Mask the cardholder's primary number (PAN) when it is displayed (SELECT), where the maximum possible number of digits to display is the first six and the last four. Example: 8600 00xx xxxx xxxx 1234	Request a selection (SELECT) from the production environment database with the presence of payment card data. Verify that card numbers are displayed in masked form.

5.3.	Apply encryption mechanisms using strong cryptographic algorithms to encrypt the full number of PAN UZCARD cards.	Request and verify DBMS settings or application settings where full PAN number encryption mechanisms are applied Also, request a selection from the production environment database with payment card data to ensure that PANs are encrypted.
5.4.	Limit access to cryptographic keys. Allow access to such keys to the smallest possible number of staff responsible for cryptographic keys. - Fully document and implement all processes and procedures for cryptographic key management for COI encryption - Generate strong cryptographic keys. - Securely distribute encryption keys. - Store encryption keys securely - Exclude unauthorized replacement of cryptographic keys.	Request a cryptographic key management document and ensure that cryptographic keys are stored securely and access to them is restricted in accordance with an internal order. Verify that the documentation is fully complied with, verify the strength of cryptographic keys, verify the security of encryption key distribution, verify the security of encryption key storage.
5.5.	Encrypt cardholder data when transmitted on open public networks 5.5.1. Use strong cryptography and security protocols to protect confidential ISP when transmitted on open public networks, subject to the following: - Only trusted keys and certificates are accepted. - The protocol used supports only secure versions and configurations. The strength of the encryption is consistent with the encryption methodology used.	Check the application configuration to ensure that data encryption is used when transmitting data over the Internet. Ensure that strong cryptography and security protocols are used to protect sensitive ISP when transmitted over open public networks.

	5.5.2 Prohibit forwarding an unsecured PAN using custom messaging technologies (e.g., email, instant messaging, text messaging, chat rooms, etc.).	
6	IMPLEMENTATION OF IB SECURITY FEATURES. 6. Implement common information security tools in the ISP environment.	

6.1.	Implement means of collecting and analyzing event logs, as well as alerting, event acquisition and correlation systems (SIEM) 6.1.1. Perform automated event logging of all system components: - Register all facts of user access to cardholder data; - Log all actions of a user with unrestricted access rights (root) and a user with administrative privileges; - Log access to all system event records; - Log all unsuccessful logical access attempts; - Log the use and modification of identification and authentication mechanisms including, but not limited to, the creation of new accounts, privilege extensions - as well as all modifications, additions, deletions to the accounts of the user with unrestricted access rights (root) or the user with administrative privileges; - Record starts, stops, or suspensions of event logging.	Check that there is a working SIEM system. Check that all servers in the ISP segment are configured to send security events to the SIEM. Check the audit settings in the system components of the partner's information system for automatic logging of security events. Make sure that only employees who need access to the event logs according to their job description have access to the event logs. Verify that event logs are stored for at least one year and in operational access for at least three months.

	6.1.2 Log at least the following parameters in the event logs for each event of each system component: User ID, Event Type, Date and Time, Whether the event was successful or unsuccessful, Event Source, Identifier or name of the data, system component or resource affected by the event. 6.1.3 Limit access to view event logs to only those employees who need such access in accordance with their job responsibilities. 6.1.4 Protect event logs from unauthorised modification. 6.1.5 Review the event logs and security events of all system components to detect anomalies or suspicious activity. Review at least once a day: - All security events - Logs of all system components that store, process, or transmit COI and/or critical authentication data - Logs of all critical system components - Logs of all servers and system components performing security functions (e.g. firewalls, intrusion detection and prevention systems, authentication servers, etc.). 6.1.6 Keep logs for at least one year, and operationally accessible for at least three months (e.g., they may be directly accessible, or archived, or may be promptly restored from backup media).	

6.2.	Install an access control system for system components that restricts access according to user need and that is configured to deny anything not previously authorized. Implement a privileged access management (PAM) system to control access to the ISP environment 6.2.1 Open access to the ISP environment with a separate account for each user with different levels of access according to an internal access matrix. 6.2.2 Enable the system to log the generation of events during PAM operation with logging of every action of all users. 6.2.3 Configure the system to send all events to the centralized system of events collection and correlation (SIEM).	Check that the PAM system is up to date. Make sure that the ISP segment servers are accessed via the PAM system. Verify that access to the ISP environment is granted by a separate account for each user with different access levels according to the internal access matrix. Ensure that the system includes a log of event generation during PAM operation with logging of every action of all users. Check that the system is configured to send all events to the centralized system.
6.3.	Implement a data leakage prevention (DLP) system to protect against confidential information leaks in the ISP environment 6.3.1 Ensure full agent coverage in user devices interacting with the ISP environment 6.3.2 Check agent activity on a daily basis, as well as alerts from the DLP system based on predefined criteria 6.3.3 Enable the system to log the generation of events when DLP Alerts occur 6.3.4 Configure the system to send all events to the centralized system for event collection and correlation (SIEM).	Verify that the DLP system is up to date. Verify that there is full agent coverage on user devices interacting with the ISP environment. Verify that there is full agent coverage on the user devices interacting with the ISP environment.

6.4.	Implement a change detection mechanism (e.g. FIM file integrity monitoring) to alert staff to unauthorized modifications (including changes, additions and deletions) to critical system files, configuration files and data files; configure software to compare critical files at least once a week. Note. In the context of change detection, critical files are files that are rarely changed but whose change may be an indication of system compromise or risk of system compromise.	Request the availability of systems, change detection mechanisms in the information systems of the ISP environment. Check that the data in the system is up-to-date and that the latest change response report is up-to-date.

	Change detection mechanisms (such as file integrity monitoring tools) usually have a predefined list of critical files in the operating system in use. Implement a process for responding to any triggering of a change detection solution.	
6.5.	Implement a system to monitor and track the status of ISP servers and services. Ensure full agent coverage on ISP servers.	Check that the status tracking and monitoring system of the ISP segment servers is up to date. Verify that there is full agent coverage of the status monitoring and tracking system on the ISP servers. Check full coverage of agents on ISP servers
7	ORGANISATION OF WORK TO ENSURE IB. 7. Organize physical, logical, methodological IS provisioning works at the Partner inclusive for the ISP environment.	

7.1.	Limit access to cardholder data as required by job duties 7.1.1 Restrict access to system components and cardholder data to only those individuals who require such access in accordance with their job duties. 7.1.2 Assign access rights based on job classification and job responsibilities. 7.1.3 Require formal approval of access by authorized parties, specifying the privileges required. 7.1.4 All access should be denied by default (set to 'deny all that is not explicitly allowed').	Verify the existence of a document or process for managing payment card data. Request supporting data on access restrictions to payment card data. Ensure that a process is in place to restrict access to system components and cardholder data to only those persons who are required to have such access by their job responsibilities.

7.2.	Ensure a password policy for the operation of the ISP environment 7.2.1 Use strong cryptography to encrypt authentication credentials (e.g., passwords/passphrases) when transmitted and stored in all system components. 7.2.2 Ensure that passwords/passphrases meet the following requirements: - password must contain at least twelve characters; - password must contain both numbers and letters. 7.2.3 Change passwords/passphrases at least once every 90 days. 7.2.4 Prohibit a user from changing his/her password/passphrase to any of the last four passwords/passphrases used by the user. 7.2.5. Install unique initial passwords/passphrases for each user and require their immediate change when the user logs in for the first time.	Ensure that there is a password management document or process in place in the ISP environment. Verify that the cryptography used to encrypt authentication credentials for transmission and storage in all system components is strong. Verify that passwords/passphrases meet the following parameters: - presence of at least twelve characters in the password; - password contains both numbers and letters. - passwords/passphrases have been changed at least once every 90 days. Install unique initial passwords/passphrases for each user and ensure that they are changed immediately when the user logs in for the first time.
7.3.	Provide multi-factor authentication (MFA) for all non-console access to the ISP environment for employees with administrator rights. Provide multi-factor authentication for all remote network access (users and administrators, including any third-party access for support or maintenance) from outside the Partner's network.	Verify that multi-factor authentication is configured for all remote network access originating from outside the Partner's network.

7.4.	Restrict access to any database containing cardholder data (including access by applications, administrators and any other users) as follows: - All database accesses, queries and operations must be performed by software methods only. - Only database administrators are allowed to query and request direct access to databases. - Only applications (and not individual users or other non-application processes) are allowed to use application identifiers.	Verify the existence of a document or process for managing access to the information systems of the ISP segment. Request supporting data on granting and restricting access to databases containing payment card data.
7.5.	Implement processes to conduct quarterly wireless point availability checks and to detect all authorized and unauthorized wireless access points. 7.5.1 Maintain a list of authorized wireless access points with the rationale for their need. 7.5.2 Implement procedures for responding when unauthorized wireless access points are detected.	Verify that a wireless management document or process is in place. Request the latest report on scanning wireless access points and detecting unauthorized wireless access points. Verify a list of authorized wireless access points is maintained, including the rationale for their need. Ensure a response procedure is implemented if unauthorized wireless access points are detected.
7.6.	Implement external and internal vulnerability scans of the network at least quarterly and after significant changes to the network. 7.6.1 Perform quarterly internal vulnerability scans. Remediate vulnerabilities and repeat scans until all 'high' risk vulnerabilities have been remediated. Scans should be performed by qualified professionals.	Verify the existence of a document or process for performing vulnerability scans of the ISP segment. Request the latest report (pages with the date and time of the scan, status of the report) of the internal vulnerability scan performed on the ISP segment.

	7.6.2 Conduct quarterly external vulnerability scans using appropriate external vulnerability scanning software. Conduct repeated scans until a satisfactory result is achieved. Scans should be performed by qualified professionals.	Request the latest report (pages showing the date and time of the scan, the status of the report) on the external vulnerability scan performed on the ISP segment.
7.7.	Implement a penetration testing methodology that: - Based on generally accepted industry approaches to conducting penetration testing - Covers the entire perimeter of the ISP environment - Provides for testing inside and outside the network - Provides for the analysis and evaluation of threats and vulnerabilities found in the last 12 months. - Regulates the storage of the results of penetration tests and the results of actions taken to remediate vulnerabilities. 7.7.1 Conduct an external penetration test at least annually and after any significant modification or upgrade of the ISP environment infrastructure. 7.7.2 Conduct an internal penetration test at least annually and after any significant modification or upgrade of the ISP environment infrastructure. 7.7.3 Remediate exploitable vulnerabilities discovered during the penetration test and retest to verify that they have been remediated.	Ensure the implementation of a penetration testing methodology that: - Based on generally accepted industry approaches to penetration testing - Covers the entire perimeter of the COI environment - Provides for testing inside and outside the network - Provides for the analysis and assessment of threats and vulnerabilities found in the last 12 months. - - Provides for the storage of penetration test results and the results of actions taken to remediate vulnerabilities.

7.8.	Implement a procedure for timely failure detection and failure notification of critical security controls that include failures: - Firewalls - Intrusion Detection and Prevention Systems (IDS/IPS) - File Integrity Monitoring (FIM) - Antivirus software - Physical access controls - Logical access controls - Audit logging mechanisms - Segmentation controls (if applicable)	Request the availability of systems, mechanisms and procedure for timely failure detection and failure notification of critical safety control systems. Verify that systems and agents for detecting failures in the information systems of the ISP segment are up to date.
7.9.	Implement a timely response to any failures of critical safety controls. Procedures for responding to failures of safety controls should include: - Restoration of safety systems functions - Identification and registration of the duration (date and time from start to end) of the failure of safety systems - Identification and registration of the cause(s) of the failure, including the root cause, and registration of the corrections required to eliminate the root cause - Identification and remediation of any security issues arising from the failure - Perform risk assessments to determine whether further action is required as a result of the failure of protection mechanisms - Implementing controls to prevent recurrence of the root cause of the failure - Resumption of security control monitoring	Verify that a document or process is in place for responding to failures of systems and servers in the ISP segment.