Joint Board Meeting
October 12, 2020

Action Item: Approve ORCA Information Security Policy

Purpose: The next generation ORCA Information Security Policy represents the commitment of ORCA management to secure ORCA information assets, protect the ORCA brand and reputation, and deliver safe, secure services to customers. It is meant to provide guidance to influence the behavior of ORCA personnel (including service providers) when performing their duties and to establish the security principles that will be embedded into ORCA operations.

Recommendation: The ORCA Business Managers recommend this Policy for approval.

ORCA Information Security Policy

Version 1.0

Revision Record

Retain v1.0 line item and the 9 most recent modifications.

Version Number	Effective Date	Entered By	Reason for Change
0.1	09/25/2020	Alan Hecker	Initial Creation
1.0			Initial Implementation

Review and Approval Record

Version Number	Reviewed By	Review Date	Approved By	Approval Date
1.0				

Contents

1. Introduction

ORCA plans, builds and operates regional transit systems and services to improve mobility for Central Puget Sound. ORCA relies on its information systems and information as essential resources to service the transportation needs of its customers. Consequently, ORCA information systems must be operated, maintained and expanded in a controlled manner. ORCA also recognizes the importance of securing the confidentiality, integrity and availability of its information assets to achieve its core mission while ensuring its continued viability and success. ORCA management is committed to implementing, supporting, enforcing and improving an information security policy that is consistent with its business objectives and mission.

1.1 Purpose

The purpose of the ORCA Information Security Policy is to provide management direction and support for ORCA information security risk management and control activities in scope of its Information Security Management System (ISMS), to ensure that they meet the ORCA information security objectives, and that they are conducted in accordance with ORCA business requirements as well as relevant laws, regulations, and standards. This Policy provides a roadmap for implementing the security controls required by Information Security Policy to protect ORCA information assets.

The Information Security Policy represents the commitment of ORCA management to securing ORCA information assets, protecting the ORCA brand and reputation and delivering safe, secure services to its customers. It is meant to provide clear guidance to influence the behavior of all ORCA Personnel (including service providers) when performing their duties, and to establish the security principles that management expects to embed into ORCA operations. This Policy is also intended to provide the necessary governance framework to support other subject-specific governance documents, organizational structures and initiatives; and to articulate the ORCA information security strategy and practices to relevant stakeholders.

2. Definitions

Agency: Each of the public transportation agencies that is a party to the ORCA Interlocal Cooperation Agreement (ILA).

Agency Personnel: Employees or service providers performing work for agencies participating in and using the ORCA system under the management of the Agency.

Compliance: The process that records and monitors the policies, procedures and controls needed to ensure adherence to established security controls and direction.

Contractor: See "**Service Provider**"

Controls: The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. Controls can be physical, technical or procedural (administrative).

Cyber Asset, Technology Asset: A technology-dependent information asset, such as programmable electronic devices and communication networks, including hardware and software.
External Entity, External Party: Any entity not affiliated with or part of ORCA.

Governance: The responsibility of Senior Management and focuses on creating the mechanisms an organization uses to ensure that Personnel follow established processes and policies. It encompasses the development and administration of policies, standards, processes and guidance to achieve ORCA's strategic objectives.

Guidelines: Documents that contain information that is helpful in executing defined procedures or meeting standards. Guidance are not prescriptive documents but, rather, reference documents that provide information that is useful in completing tasks.

Information Assets: All organizational assets that may generate, process, store, or transmit information, including the information itself.

Information Processing Facility: A physical facility that houses information systems or its virtual equivalent.

Information Security: Ensuring the confidentiality, integrity and availability of information.

Information Security Management System (ISMS): An Information Security Management System consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an

organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

Information Security Manager: The employee of the ROOT who serves as the technical expert in the evaluation of all proposed actions and activities that may have an impact on the security of the ORCA System.

Information Security Program (ISP): The overall combination of technical, operational and procedural measures, and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis.

Information System: A cyber asset that is also an information asset.

Information: Data, knowledge and/or records that are required by an organization to fulfill its mission and achieve its objectives.

Joint Board: The governing, policy-setting body that oversees the activities of the ORCA System as described under the ORCA System Interlocal Cooperation Agreement (ILA).

Management: Leadership of the ROOT's Information Security policies and practices, including the ORCA Director and/or the ROOT Information Security Manager.

ORCA Director: Employee of the ROOT, approved by, and reporting to the Joint Board, who directs and oversees the administration, operations, and planning of the ORCA System.

ORCA System: The equipment, systems, facilities, ORCA cards, ORCA products, websites, data, information, and any products and services implemented by the ORCA agencies using smart cards, open architecture and application-based systems to provide fare payment on ORCA agency transportation services.

ORCA Personnel: Employees and Service Providers performing work for ORCA under ORCA management and direction.

Policies: The high-level statements of management intent, expectations and direction. ORCA Policies may be adopted or amended by the Joint Board or ORCA Director.

Procedures: A detailed, step-by-step set of directions required to complete a specific task or activity, in order to meet the requirements of applicable standards.

Processing Facilities: An information processing facility is any system, service, or infrastructure, or any physical location that houses these things. A facility can be either an activity or a place and it can be either tangible or intangible.

Regional Chief Information Security Officer (CISO): The senior-level executive responsible for establishing and maintaining the enterprise vision, strategy and program to ensure ORCA information assets and technologies are properly protected.

Risk Management: The process by which an organization sets the risk tolerance, identifies potential risks and their associated impacts, and prioritizes their mitigation based on the organization's business objectives and risk tolerance. Risk Management develops and deploys internal controls to manage and mitigate risk throughout the organization.

ROOT: Regional ORCA Operations Team.

Senior Management: the leadership of the ROOT, including ORCA executive leadership.
Service Provider, Supplier, Third Party, Vendor, Contractor: Any outside entity that is providing goods or services to ORCA.

Standard: Standard, in the context of Information Security, are the metrics, allowable boundaries or the criteria used to determine whether procedures, processes or systems meet policy requirements. Standard documents provide guidance on how to implement the vision in a policy statement.

Technology Asset: See "**Cyber Asset**."

Technology: Any piece of equipment that is developed through the application of scientific knowledge that accomplishes its objectives through the use, processing or transmittal of information in electronic form.

3. Scope

3.1 In Scope

All applications, Information in electronic format, Information Systems and Information Processing Facilities owned and/or operated by the ROOT, as well as third-party provided Information Systems and Information processing services (for applicable provisions). . Each Agency will adopt policies that are consistent with this policy and may use different approaches to achieve the specific control objectives outlined in this document.

3.2 Out of Scope

Applications and systems that are owned and operated by the Agencies and not part of the ORCA System are out of the scope of this Policy.

4. Intended Audience

4.1 Primary Audience

1. ORCA and Agency Personnel responsible for Information Systems and Information Processing Facilities.
2. ORCA Personnel responsible for the operation of the ORCA Information Security Management System (ISMS) and Information Security Program.
3. ORCA and Agency Personnel responsible for designing and operating processes and systems with an impact on information security controls.
4. Agency Personnel responsible for the development and implementation of Agency security and compliance programs and policies.
5. Service providers that are contractually required to align with the ORCA ISMS.
6. Internal and external information security and compliance auditors.
7. External stakeholders interested in ORCA Information Security posture.

4.2 Secondary Audience

Other ORCA functions with a role in supporting information security controls.

5. Objectives

5.1 General Objectives

1. To provide Management direction in expected practices impacting ORCA Information Security posture.
2. To support the achievement of ORCA Information Security objectives, identified by the ORCA Information Security Management System (ISMS).
3. To articulate ORCA Information Security practices to relevant internal and external stakeholders.
4. To ensure that core areas of ORCA activities are adequately addressed from an Information Security perspective.
5. To provide governance support for the operation of ORCA Information Security Management System (ISMS) as a key component of its Information Security Risk Management strategy.
6. To align with industry recognized best practices in the Information Security field, such as ISO 27001:2017.

5.2 Specific Objectives

5.2.1 Management

1. To provide management direction and support for Information Security in accordance with business requirements and relevant laws and regulations.
2. To establish a management framework to initiate and control the implementation and operation of Information Security within ORCA.
3. To ensure that Information Security is implemented and operated in accordance with ORCA Policies and Procedures.

5.2.2 Protection of Information and Facilities

1. To ensure that Information receives an appropriate level of protection, in accordance with its importance to ORCA.
2. To protect against the loss of data by preventing unauthorized disclosure, modification, removal or destruction of Information stored on digital media.
3. To protect against loss of data.
4. To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of ORCA Information.
5. To ensure that Information and Information Processing Facilities are protected against malware.
6. To ensure the protection of Information in ORCA networks and its supporting Information Processing Facilities.

7. To ensure correct and secure operations of Information Processing Facilities.

5.2.3 Availability

1. To ensure availability of ORCA Information Processing Facilities.

5.2.4 Access

1. To control physical and electronic access in order to prevent unauthorized access, damage and interference to ORCA Information and Information Processing Facilities.
2. To prevent unauthorized access to systems and applications.

5.2.5 Operational Systems

1. To ensure the integrity of ORCA Systems.
2. To minimize the impact of audit activities on ORCA operational systems.
3. To record events related to Information Systems and generate evidence.

5.2.6 Assets

1. To ensure ORCA Information Assets are identified and that appropriate protection and responsibilities are defined.
2. To prevent loss, damage, theft or compromise of Information Assets and interruption to ORCA operations.
3. To ensure the security of teleworking and use of mobile devices.

5.2.7 External Service Providers

1. To ensure protection of ORCA Information Assets that are accessible by service providers.
2. To maintain the security of Information transferred within ORCA and with any external entity.
3. To maintain an agreed level of Information Security and service delivery in line with service provider agreements.

5.2.8 Personnel

1. To ensure that Personnel understand and remain aware of their Information Security responsibilities, and are suitable for the roles for which they are considered.
2. To protect ORCA interests as part of the process of changing or terminating employment.
3. To ensure users are accountable for safeguarding their authentication information.

5.2.9 Lifecycle

1. To ensure that Information Security is an integral part of ORCA Information Systems across the entire lifecycle.
2. To ensure that Information Security is designed and implemented within the development lifecycle of ORCA Information Systems
3. To ensure the protection of data used for testing

5.2.10 Incidents

1. To ensure a consistent and effective approach to the management of Information Security incidents, including communication on security events and weaknesses.
2. To avoid breaches of legal, statutory, regulatory or contractual obligations related to Information Security and of any security requirements.
3. To ensure that Information Security continuity is properly incorporated in ORCA business continuity management systems.

6. Compliance

These requirements are effective as of the date of this Policy is adopted or amended by the Joint Board.

7. Exceptions

Due to operational and business needs, it is possible that exceptions to this Policy or related governance may be required. Exception requests must be channeled through the Information Security Manager, along with business justification and information on applicable mitigating controls, for evaluation and regional CISO recommendation of approval. Authority to grant exceptions lies with the Joint Board and they may delegate it to other regional functions, as appropriate based on the level of risk.

All exceptions to these requirements will have a maximum duration of one year. Requests to extend the validity of a standing exception must be submitted one month prior to the expiration of the exception, with sufficient information to establish the continued business needs.

In certain circumstances, the Joint Board may authorize an exemption to a specific security control upon recommendation by the Regional CISO, provided that: a) there are adequate compensating controls being implemented and b) there is a documented risk acceptance from the respective risk owner on record. As with exceptions, additional approval by ORCA Director may be required prior to presenting the exemption to the Joint Board, based on the level of risk to ORCA posed by the exemption.

8. Document Maintenance

This document is reviewed and/or updated annually, or more frequently as dictated by ORCA needs. Any changes must be presented to the Joint Board for approval, along with the Regional CISO's assessment of the security impact of the changes, in compliance with this Policy. The document custodian responsible for its maintenance will be the ROOT Information Security Manager.

9. Roles and Responsibilities

9.1 Management

Management is responsible for ensuring that the objectives and plans for the ISMS are established and reviewed annually, that the roles and responsibilities regarding information security are defined, that awareness programs are conducted, that an internal audit is conducted at least once a year, and that the necessary resources to maintain and improve the ISMS are provided.

9.2 Regional CISO

The Regional CISO is responsible for overseeing and supporting all aspects of the organization's information security. They decide on all the requirements for the effective operation of the ISMS by means of administrative directives, previously submitted to the ORCA Director and the Joint Board.

9.3 ROOT Information Security Manager

The Regional Information Security Manager carries out the directives of the Joint Board, ORCA Director, and CISO with regard to the ISMS.

10. Information Security Requirements by Control Area

This Policy requires the following requirements to be properly addressed, for each one of the listed control areas in scope:

10.1 Policy Development and Maintenance

In order to provide management direction and support for Information Security in accordance with business requirements and relevant laws and regulations, the approach on this control area is to:

1. Publish rules of behavior governing Information Systems.
2. Develop, disseminate and annually review/update Information Security governance standards to support the implementation of the statements and objectives in its Information Security policy and strategy.
3. Establish a regional Information Security Management System (ISMS) to manage ORCA information security risks.
4. Maintain an Information Security Program (ISP) that aligns with, supports and helps achieve ORCA business goals. The ISP is the instrument to execute and implement the Information Security controls in scope of ORCA ISMS.
5. Develop, implement and subsequently assess, on an annual basis, ORCA overall Information Security Program, including planning documents.
6. Evaluate ORCA Information Security governance and controls to determine if they are implemented correctly, operating as intended, and producing the desired outcome in achieving ORCA Information Security goals.
7. For Information Systems as specified by ORCA management, develop, document, and maintain (as appropriate):
    a. Current baseline configurations.
    b. Types of changes that are configuration-controlled.
    c. Physical and logical access restrictions associated with changes.
    d. Mandatory configuration settings.
    e. Inventory of Information System components.
    f. Configuration management plan.

10.2 Organization of Information Security

ORCA approaches the *Organization of Information Security* control area as follows:

10.2.1 Internal Organization

1. Identify and allocate specific Information Security roles and responsibilities.
2. Identify applicable legal, regulatory or compliance requirements for each technology and/or system used.

3. Implement processes designed to ensure that applicable Information Security requirements are aligned with ORCA business needs and strategy, and are adequately enforced.
4. Implement segregation of duties for conflicting duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of ORCA Information assets (including data) and technology.
5. Maintain contacts with authorities relevant to ORCA Information Security posture.
6. Maintain contacts with special interest groups, specialty security forums and professional associations in the Information Security field.
7. Ensure that Information Security requirements are addressed as part of project management practices.
8. Plan and coordinate security-related reviews affecting Information Systems throughout their development and operational life cycles, including acquisition of third-party or cloud-based computing solutions.
9. Maintain a comprehensive strategy to manage Information Security risk to organizational operations and ORCA Information Assets.
10. Maintain, review and update an Information Security Risk Register to ensure that risks are adequately assessed and managed.
11. Direct risk assessment activities, reviews and updates as needed to support the operation of the Information Security Management System.

10.2.2 Mobile Devices and Teleworking

ORCA approaches the *Mobile Devices and Teleworking* control area as follows:

1. Establish governance to manage risks introduced by the use of mobile devices.
2. Establish governance to protect ORCA Information accessed, processed or stored at teleworking sites devices or accessed by mobile devices.

10.2.3 Human Resources Security

ORCA approaches the *Human Resources Security* control area as follows:

1. Prior to Employment
    a. Conduct background verification checks on all candidates for employment, in accordance with relevant laws and regulations; proportional to ORCA business requirements, the classification of the information to be accessed and the perceived risks.
    b. Ensure that contractual agreements with contractors and consultants include ORCA and their responsibilities for Information Security.
    c. Require System users to complete a user agreement prior to granting Information System access.

2. During Employment

    a. Implement and enforce mechanisms to ensure that Information Security breaches involving Personnel are appropriately addressed and resolved.
    b. Require Personnel to observe Information Security guidance in accordance with ORCA applicable Policies, Standards and Procedures.
    c. Provide basic Information Security awareness training to all Information System users, and regular updates in ORCA Policies and Procedures, as relevant for their job function, at least annually.
    d. Provide additional Information Security training materials based on specific roles and responsibilities, as determined by ORCA Management and compliance requirements.
    e. Document and monitor Information System security training activities.
    f. Document and implement segregation of duty (SOD) rules, for sensitive roles, as determined by ORCA Management.
    g. Only grant Personnel those access privileges that are necessary to accomplish assigned tasks (Least Privilege Principle).
    h. Display appropriate notification messages or banners before granting access to its systems (as appropriate), whenever technically feasible.

3. Termination and Change of Employment

    a. Implement processes to address changes to employment or engagement status that may have an impact on ORCA Information Security posture.
    b. Define requirements to reevaluate ORCA Information System access upon user change of job position or responsibilities.
    c. Terminate Personnel access to ORCA Information Systems within a defined window upon the termination of employment or Personnel engagement.
    d. Define, communicate to Personnel, and enforce any Information Security responsibilities and duties that may remain valid after termination or change of employment.

10.2.4 Asset Management

ORCA approaches the *Asset Management* control area as follows:

1. Responsibility for Assets

    a. Maintain an asset register that contains details on ORCA Information Assets.
    b. Ensure that Information Assets associated with Information and Information Processing Facilities are identified, and that proper inventories of these Information Assets are prepared and maintained.
    c. Ensure that Information Assets in the asset register and/or other inventories have identified and documented business owners.
    d. Identify, document, implement and disseminate rules for the acceptable use of Information and of Information Assets associated with Information and Information Processing Facilities.

e. Develop and implement Processes to ensure that all Personnel and external party users return all ORCA Information Assets in their possession upon termination of their employment, contract or engagement; unless otherwise authorized by ORCA Management.

2. Information Classification

    a. Develop and implement a data classification and protection Standard to classify ORCA Information in terms of applicable legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
    b. Develop and implement a Standard to handle and protect Information Assets in accordance with the Information classification scheme adopted by ORCA.

3. Media Handling

    a. Restrict access to media to appropriate Personnel, in a manner that is consistent with applicable ORCA Standards for the data stored in such media.
    b. Protect and control media during transport outside of controlled areas, in a manner that is consistent with the applicable data classification and protection standards for the Information stored in such media.
    c. Employ sanitization methods on media, prior to disposal.
    d. Address control methods relevant to removable digital media devices.

10.2.5 Access Control

ORCA approaches the *Access Control* area as follows:

1. Business Requirements of Access Control

    a. Develop, document, implement and review access control Standards for access to ORCA Information and Information Processing Facilities, based on ORCA business and Information Security requirements.
    b. Ensure that Personnel are only provided with access to the network and network services that they have been specifically authorized to use.

2. User Access Management

    a. Develop and implement a formal user registration and de-registration process to enable assignment of access rights to ORCA Information Systems.
    b. Develop and implement a formal user access provisioning to assign or revoke access rights for all user types to all ORCA Systems and services.
    c. Define requirements for granting access to third party users of ORCA Information Systems.
    d. Restrict and control the allocation and use of privileged access rights to ORCA Information Systems.
    e. Develop and implement a formal management Process to allocate secret authentication information.

f. Manage all Information System accounts and account-related processes, for business critical Systems as defined by ORCA Management.
g. Use and enforce account definition parameters and settings to constrain and control account usage, as dictated by ORCA security strategy for the Information Asset.
h. Limit system administration tasks and duties to authorized and approved Personnel.
i. Manage Information Systems identifiers and authenticators for both users and devices.
j. Implement controls designed to ensure that ORCA Information Systems uniquely identify and authenticate users before establishing a connection or allowing access, when technically feasible.
k. Ensure that ORCA Information Systems obscure feedback of authentication Information during the authentication process, whenever technically feasible
l. Ensure that logical access authorizations to Information Systems are periodically reviewed.

3. User Responsibilities

    a. Develop and disseminate guidance to Personnel on ORCA Standards on the use of secret authentication information.

4. System and Application Access Control

    a. Restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.
    b. Restrict access to program source code for ORCA Information Systems.
    c. Control access to ORCA Information Systems and applications via a secure log-on procedure, as required by the access control and any other applicable Standards.

10.2.6 Cryptography

ORCA approaches the *Cryptography* control area as follows:

1. Cryptographic Controls

    a. Develop, document and implement a Policy on the use of cryptographic controls for the protection of ORCA Information, including guidance on the use, protection and lifetime of cryptographic keys.

10.2.7 Physical and Environmental Security

ORCA approaches the *Physical and Environmental Security* control area as follows:

1. Secure Areas

    a. Develop, document, implement, and disseminate a hosting Standard for its Information Assets.
    b. Define and use security perimeters to protect areas that contain either sensitive or critical Information Systems.
    c. Control physical access to ORCA Information Processing Facilities.

d. Develop and implement controls that are designed to ensure that ORCA protects its Information Systems from loss or damage resulting from theft, power loss, heat, water or fire.
e. Develop, document, implement and disseminate Procedures for working in designated secure areas.

2. Equipment

a. Follow sound security practices and all applicable ORCA Procedures when performing maintenance activities.
b. Control and monitor the use of Information System maintenance tools.
c. Periodically review physical access authorizations to Information Systems/Information Processing Facilities to assess compliance with applicable ORCA Standards.
d. Protect its technology infrastructure in a way that is commensurate with the value and criticality of the supported Information Systems.

10.2.8 Operations Security

ORCA approaches the *Operations Security* control area as follows:

1. Operational Procedures and Responsibilities

a. Document operating Procedures and make them available to all Personnel who need them to perform their function.

b. Ensure that changes to ORCA business Processes, Information Processing Facilities and Systems that affect Information Security are properly managed and controlled.
c. Assess changes to Information Systems to determine potential security impacts prior to implementation.
d. Manage the use of its technology resources and available capacity to ensure that the required System performance is adequate to meet ORCA needs.

2. Protection from Malware

a. Implement detection, prevention and recovery controls to protect against malware when technically feasible, combined with appropriate user awareness.
b. Deploy malicious code protection mechanisms at Information System entry and exit points and computing devices, when technically feasible.

3. Backup

a. Maintain adequate backup copies of Information, software and System images to enable recovery from Information Security incidents, in accordance with applicable ORCA Standards and business needs.

4. Logging and Monitoring

a. Produce, keep and regularly review event logs recording user activities, exceptions, faults and Information Security events affecting ORCA Information Systems, as specified by ORCA Management.
b. Protect logging facilities and Information system log Information against tampering and unauthorized access.
c. Produce, keep, protect and regularly review logs recording system administrator and system operator activities involving ORCA Information Systems, as specified by ORCA Management
d. Synchronize the clocks of all relevant Information processing systems within a security domain to a single reference time source, when technically feasible.
e. Deploy a continuous monitoring strategy and monitoring program to monitor connections involving business critical Information Systems (as determined by ORCA Management) on an ongoing basis, verifying enforcement of security requirement.
f. Determine the appropriate monitoring level for each Information System.

5. Control of Operational Software

    a. Implement Procedures to control the installation of software on the ORCA System.

6. Technical Vulnerability Management

    a. Establish a technical vulnerability management capability to ensure that the exposure of ORCA Information Systems to such vulnerabilities is evaluated and appropriate measures are taken to address the associated risks.
    b. Establish adequate service level agreements for remediation of vulnerabilities, in alignment with the risk appetite set for the ORCA System.
    c. Establish and implement rules governing the installation of software by users.

7. Information Systems Audit Considerations

    a. Carefully plan any audit requirements and activities involving verification of operational Systems to minimize disruptions to critical business Processes.
    b. Determine which Information Systems must be capable of auditing and reporting.
    c. Establish what are considered sufficient levels and amounts of audited Information.
    d. Adequately allocate and monitor audit record storage capacity.
    e. Enable alert mechanisms for audit processing failures.

    f. Employ mechanisms to ensure the file integrity, and monitoring to detect unauthorized changes.

10.2.9 Communications Security

ORCA approaches the *Communications Security* control area as follows:

1. Network Security Management

    a. Ensure that ORCA networks are properly managed and controlled to protect Information in Systems.
    b. Ensure that security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether they are provided in-house or outsourced.
    c. Ensure that Information services, users and Information Systems are adequately segregated on networks, according to best design practices and their specific functions.
    d. Define essential functionality such that non-essential functionality is disabled or removed on Information Systems designated by ORCA Management.
    e. Employ secure strategies for network connection session management.
    f. Implement controls designed to ensure that Systems with external connections are protected by hardening, monitoring (e.g. Intrusion Detection/Prevention technologies) and firewalling functionality (or approved equivalent).
    g. Implement controls designed to ensure that all external connections to ORCA networks are registered with and approved by ROOT.

    h. Implement controls designed to ensure that approved authorizations exist for all access to ORCA Information Systems and for controlling the flow of Information within the System and between interconnected Systems.

2. Information Transfer

    a. Establish governance and controls to protect the transfer of Information through the use of all types of communication facilities.
    b. Ensure that agreements address the secure transfer of business Information between ORCA and external parties.

    c. Adequately protect Information involved in electronic messaging.
    d. Identify, regularly review and document requirements for confidentiality or non-disclosure agreements that reflect ORCA needs for the protection of Information and applicable laws and regulations.

10.2.10 Information Systems Acquisition, Development and Maintenance

ORCA approaches the *Information Systems Acquisition, Development and Maintenance* control area as follows:

1. Security Requirements of Information Systems

a. Include Information Security related requirements into the overall requirements for new Information Systems or enhancements to existing Information Systems.
b. Implement reasonable measures to protect ORCA Systems and Information from threats that could compromise their confidentiality, integrity and availability.
c. Implement isolation techniques, separate physical domains, perimeter controls, and a layered security approach ("defense in depth", as appropriate) to address unauthorized access to Information, Systems or other technology resources.
d. Implement security mechanisms to protect ORCA Information and Information Assets, commensurate with their value and sensitivity.
e. Protect Information involved in application services passing over public networks from fraudulent activity, repudiation and unauthorized disclosure and modification.
f. Protect Information involved in application service transactions to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
g. Address emerging communication and networking technologies for their Information Security implications prior to incorporation into ORCA technology portfolio.
h. Implement controls designed to ensure that system and services acquisition standards and procedures reflect key information security requirements.

i. Ensure that contracts for the procurement of Information Systems or Information hosting or processing services include terms to address Information Security considerations.
j. Obtain and make available to authorized Personnel appropriate Information Systems documentation.

2. Security in Development and Support Processes

a. Establish and apply rules for the development of software and systems, to developments within ORCA.
b. Control changes to systems within the development lifecycle by the use of formal change control procedures.
c. Review and test business critical applications whenever operating platforms are changed, to ensure there is no adverse impact on ORCA operations or security.
d. Establish, document, maintain and apply to any information system implementation efforts, principles for engineering secure systems.
e. Establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
f. Supervise and monitor the activity of outsourced system development.
g. Carry out testing of security functionality during development.
h. Establish acceptance testing criteria and methodologies for new information systems, upgrades and new versions.

3. Test Data

    a. Carefully select, protect and control test data.
    b. Incorporate security considerations and identification of security roles and responsibilities into the System development lifecycle process.
    c. Implement processes designed to ensure that software installation, maintenance and administration are restricted to authorized Personnel.
    d. Implement controls designed to ensure that ORCA Information Systems use mechanisms for authentication to cryptographic modules that meet prevailing industry Standards and best practices, when technically feasible.
    e. Establish and manage cryptographic protection processes and keys.
    f. Direct risk assessment activities, reviews and updates.
    g. Identify, report, and correct Information System flaws.
    h. Incorporate into standard operations Information System security alerts, advisories, and directives from designated external organizations on an ongoing basis.
    i. Monitor events on ORCA Information Systems according to Information Security objectives; with the goal of detecting Information System attacks.
    j. Define and enforce minimum security configuration standards for servers and other critical systems, as defined by ORCA Management.
    k. Manage Information within and output from ORCA Information Systems according to applicable requirements, laws and regulations.
    l. Create an action plan to correct weaknesses and vulnerabilities and identifying issues during assessments.

10.2.11 Supplier Relationships

ORCA approaches the *Supplier Relationships* control area as follows:

1. Information Security in Supplier Relationships

    a. Ensure that information security requirements for mitigating the risks associated with a supplier's access to ORCA information assets or information are agreed with the supplier and properly documented.
    b. Ensure that all relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate or provide IT infrastructure component's for ORCA information.
    c. Ensure that agreements with suppliers include adequate requirements to address the information security risks associated with information and communications technology services and the product supply chain.

2. Supplier Service Delivery Management

    a. Monitor and review the performance of ORCA supplier service delivery, for services impacting ORCA information or systems.

    b. Manage the changes to the provision of services by suppliers, considering the criticality of the information, systems and processes involved, and reassessing applicable risks.

10.2.12 Information Security Incident Management

ORCA approaches the *Information Security Incident Management* control area as follows:

1. Management of Information Security Incidents and Improvements

    a. Maintain an Information Security Incident Response Plan and an Information Security Incident Handling capability. The plan shall:
        - Establish management responsibilities and procedures as part of the Information Security Incident Response Plan to ensure a quick, effective and orderly response to information security incidents.
        - Outline the criteria to assess information security events and determine their classification as information security incidents.
        - Establish a process to use knowledge gained from analyzing and resolving information security incidents to reduce the likelihood or impact of future incidents.
        - Define procedures to be applied for the identification, collection, acquisition and preservation of information, which can serve as evidence associated with an information security incident.

    b. Develop, disseminate and annually review/update the incident response process and supporting documents.

    c. Observe applicable documented procedures when responding to information security incidents.

    d. Ensure all incidents involving ORCA information are reported to ORCA Information Security.

    e. Require Personnel using ORCA information systems and services to note and report any observed or suspected information security weaknesses in systems or services.

    f. Track and document all information system security incidents.

    g. Train ORCA Personnel on their incident response roles and responsibilities, as applicable.

    h. Test and/or exercise the incident response capability periodically.

    i. Inform users that ORCA reserves the right, in its discretion and without Personnel permission, to review any documents or electronic files created by or stored on ORCA systems, as well as Personnel's voice or e-mail messages and Internet usage to the extent necessary to ensure that electronic systems are being used in compliance with the law and with ORCA policies, as well as investigating information security incidents. **Personnel privacy does not extend to Personnel's work-related conduct or to the use**

of ORCA-provided equipment or supplies. Therefore, Personnel should never assume electronic communications are entirely private and confidential.

j. Establish rules of engagement for incident investigation and forensic activities involving computing devices used by Personnel in connection with ORCA activities, including scope, roles and responsibilities, in accordance with applicable law.

10.2.13 Business Continuity Management

ORCA approaches the *Business Continuity Management* control area as follows:

1. Ensure that the impact of Business Continuity is assessed by ORCA information security risk management practices.

10.2.14 Information Security Aspects of Business Continuity

ORCA approaches the *Information Security Aspects of Business Continuity* control area as follows:

1. Information Security Continuity
    a. Determine the requirements for information security and the continuity of information security management during a crisis or disaster situation.
    b. Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

2. Redundancies
    a. Develop and execute a strategy to ensure that systems supporting critical business processes, as defined by ORCA management, can be recovered in the event of a disaster.
    b. Incorporate business continuity and disaster recovery considerations into the annual planning of the ORCA technology portfolio.

    c. Implement information processing facilities and systems with redundancy that is sufficient to meet availability requirements established for the information services and business processes being supported.

10.2.15 Compliance

ORCA approaches the *Compliance* control area as follows:

1. Compliance with Legal and Contractual Requirements

a. Identify, document and keep up to date all relevant legislative statutory, regulatory, contractual requirements related to information security, and ORCA approach to meeting such requirements.
b. Identify information systems subject to specific legal, regulatory or compliance requirements and implementing a process to ensure compliance.
c. Implement appropriate procedures to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
d. Protect records from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.
e. Ensure the privacy and protection of personally identifiable information as required in relevant legislation and regulations, where applicable.
f. Ensure that cryptographic controls are used in compliance with all relevant agreements, legislation and regulations.

2. Information Security Reviews

a. Ensure independent reviews of ORCA approach to managing information security and its implementation (including control objectives, controls, policies, processes and procedures), at planned intervals or when significant changes occur.
b. Ensure that managers and supervisors regularly review the compliance of information processing and procedures within their area of responsibility, with the appropriate policies, standards and any other applicable security requirements.
c. Regularly review information systems for compliance with ORCA information security policies and standards.

11. References

ISO/IEC 27001:2017 – “Information Technology – Security Techniques – Information Security Management Systems – Requirements”
ISO/IEC 27002:2017 – “Information Technology – Security Techniques – Information Security Management Systems – Controls”
ISO/IEC 27003:2017 – “Information Technology – Security Techniques – Information Security Management Systems – Guidance”
ISO/IEC 27005:2011 “Information Technology – Security Techniques – Information Security Risk Management”
NIST 800-53 rev 4. “Security and Privacy Controls for Federal Information Systems and Organizations”
NIST Cybersecurity Framework
PCI DSS v3.2 “Payment Card Industry – Data Security Policy”
ISACA “CISM Review Manual”