Date of Issue	Standard Operating Procedure Subject:	
31st March 2023	Information Security Policy	2022/SOP/001/01

Proposed By:	Verified By:	Approved By:
Chiranjeevi Venkata	Snehashis Ghosh	Amit Sukhija
Infrastructure & Security Lead	Director – Digital Solutions	Founder & CEO
10th April 2022	10th April 2022	10th April 2022

Date of Issue	Standard Operating Procedure Subject:	
31st March 2023	Information Security Policy	2022/SOP/001/01

1.0 INTRODUCTION

ZESTIOT and ZESTIOT employees have an inherent responsibility to protect the physical information assets of the company as well as confidential member's data and intellectual assets owned by the company. These critical assets must be safeguarded to mitigate any potential impacts to ZESTIOT and ZESTIOT's members. Information Security at ZESTIOT is, therefore, a critical business function that should be incorporated into all aspects of ZESTIOT.'s business practices and operations.

To achieve this objective, policies, procedures, and standards, have been created to ensure secure business practices are in place at ZESTIOT. Information security is a foundational business practice that must be incorporated into planning, development, operations, administration, sales and marketing, as each of these business functions requires specific safeguards to be in place to mitigate the risk associated with normal business activities.

ZESTIOT is subject to numerous Government IT Security, Privacy laws and regulations, which if not complied with, could potentially result in fines, audits, reputational loss and direct financial impacts to the company. Compliance with all applicable regulations is the responsibility of every employee at ZESTIOT.

Date of Issue	Standard Operating Procedure Subject:	
31st March 2023	Information Security Policy	2022/SOP/001/01

2.0 INFORMATION SECURITY POLICY OVERVIEW

Everyone at ZESTIOT is responsible for familiarizing themselves with and complying with all ZESTIOT.'s policies, procedures and standards dealing with information security.

2.1 Definition of Information Security

Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security.

2.2 Why Security?

ZESTIOT requires information security to protect information assets from security threats. It is critical to protect the system environment to maintain a competitive advantage, to ensure profitability, and to secure and maintain member and partner trust and confidence.

Security threats originate at a wide variety of sources, including computer-assisted fraud, industrial espionage, sabotage, vandalism and natural disasters. Computer viruses, unethical hacking and denial of service attacks are examples of threats encountered while operating over the Internet. These types of threats are becoming increasingly more common, more ambitious and more sophisticated.

ZESTIOT.'s philosophy of protection provides the intent and direction behind our protection policies, procedures, and control. Our protection philosophy is comprised of three tenets:

ZESTIOT Approach:

Security is everyone's responsibility. Maintaining an effective and efficient security posture for ZESTIOT require a proactive stance on security issues from everyone. Security is not "somebody else's problem;" as a member of ZESTIOT you have the responsibility to adhere to the security policies and procedures of the company and to take issue with those who are not doing the same.

Security permeates the ZESTIOT organization. Security is not just focused on physical and technical, ZESTIOT seeks to ensure reasonable and appropriate levels of security awareness and protection throughout our organization and infrastructure.

A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within the marketplace and must be treated as a valued commodity.

The following factors are critical to the successful implementation of security within ZESTIOT:

- Comprehensive security policies, objectives and initiatives that clearly reflect ZESTIOT business objectives

- A security approach that is consistent with ZESTIOT's culture
- Highly visible support from ZESTIOT's executive management
- Complete understanding of security requirements and risk management practices
- Effective communication of security to all ZESTIOT managers, associates, partners, clients, vendors, and developers
- Guidance on information security policy to all ZESTIOT managers, associates, partners, clients, vendors, and developers
- Information security awareness and training
- Continual review and measurement of the effectiveness and efficiency of security controls and mechanisms
- Timely adjustments to the security posture by addressing deficiencies and by reflecting changes in ZESTIOT.'s business objectives as necessary
- Annual review of the information security policy to update policy as needed to reflect changes to business objectives or the risk environment.

Information Security Policy Structure

ZESTIOT's Information Security Policies are structured in such a way to give flexibility as required by the business objectives and needs while maintaining a 'level playing field' across the company. Frequently, the weakest link is the link that breaks the security chain and causes a breach in security. Through consistent application of Information Security across the company, any weak areas are compensated for, and the organization is stronger overall.

Information Security Policy follows this tiered structure:

Information security Mission Statement

Information Security Policy

Information Security Standards, Processes, and guidelines

Information Security Specific Configurations and Procedures

The hierarchy lends support as you progress up the tiers and becomes more detailed as you progress down the tiers. In this way, all actions taken have a basis in policy and directly support the policy or policies they are governed by. To illustrate this hierarchy, descriptions of the various levels are given below.

Date of Issue	Standard Operating Procedure Subject:	
31st March 2023	Information Security Policy	2022/SOP/001/01

Information Security Mission Statement – This is the overall management direction regarding Information Security at ZESTIOT. It is broad in scope and sets the expectations for protecting the company's information resources. It is contained in this document.

Information Security Policy – This is the collection of policies that implement the overall guidance of the Mission Statement. Policies are somewhat broad but topical in nature (centered on specific Information Security topics). ZESTIOT's Information Security Policies are organized in accordance with ISO 27001, Information Technology – Code of Practice for Information Security Management, an international standard and follows other regulatory and compliance mandates where applicable. Policies apply equally to everyone within the company, regardless of location. The Information Security Policies are contained in this document.

Information Security Standards, Processes, and guidelines – These are collections of standards, processes and guidelines that are to be used to implement the given policy they reference. Standards may dictate a type of technology to use but may stop before naming a product (depending on the policy and standard subject). Processes will detail the steps to take to fulfill the goals of a policy. Standards and Processes will be published under separate titles and may be regionalized to fit the conditions at different locations. The set of instructions will be published to achieve the process will be comes under guidelines.

Information Security Specific Configurations and Procedures – These are very specific details that support the implementation of the standards and processes given above. These will include specific products and configuration details, or step-by-step procedures to implement processes. These are very highly localized and will apply to the environment for which they were written.

Information Security Policy Document – ZESTIOT Executive Management will provide direction for, approve, publish, and communicate the merits of an Information Security Policy document. This Information Security Policy Document shall outline management's approach to Information Security as well as providing the organization with a strong indication of the management's commitment to Information Security within ZESTIOT.

Explain the organization's security policies, standards, and compliance requirements, including:

Compliance with legislative and contractual requirements,

Security education and awareness commitment,

Consequences for security violations.

Prevention and protection against viruses and other malicious software attacks,

Commitment to well thought-out and effective business continuity management.

Outline specific responsibilities for information security management.

Outline policies and procedures for reporting security incidents.

The Director – Digital Solutions shall be the owner of this Information Security Policy Document. The owner of the document shall be responsible for maintaining and reviewing the policy based upon a defined review process. The policy shall be reviewed at least annually and updated in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new regulations, or changes to the organization's infrastructure.

The reviews shall include an assessment of the policy's effectiveness based upon:

The nature and number and impact of recorded security incidents.

Cost and impact of controls on business efficiency; and

Effects of changes to technology.

Security Organization

Information Security Infrastructure

Allocation of Information Security Responsibilities

The Director – Digital Solutions is responsible for the overall application of the Information Security policies.

Each individual location will have a location manager who is responsible for the overall application of the Information Security Program and policies at that site.

Each asset will have an "owner", who may delegate responsibilities, but remains ultimately responsible for the asset(s).

The asset owner will:

Identify and define all security processes for their asset(s);

Document all security processes on their assets; and

Clearly define and document all authorization levels of their assets

Authorization Process for Information Processing Facilities

The authorization process for new Information Processing facilities requires that the Director – Digital Solutions perform a risk assessment prior to authorizing a new Information Processing facility. This risk assessment should follow a standard format or checklist.

The results of the risk assessment will be incorporated to establish additional controls by ZESTIOT's Security and the location manager.

External Parties

ZESTIOT may obtain the services of outside security experts, as necessary, to protect the information assets within the organization by co-coordinating in-house knowledge and experiences to ensure consistency, provide guidance in decision making, and assess the overall effectiveness of ZESTIOT's Security policy.

All use of outside security experts shall be coordinated with the Director – Digital Solutions before such experts are employed by ZESTIOT in any capacity.

All contact and cooperation with third parties on security matters will be coordinated through the Director – Digital Solutions.

The Security lead shall maintain a list of contacts with:

- The law enforcement community
- The regulatory community
- Information service providers
- Telecommunications operators
- The Security lead should also maintain contact with security forums and other notification agencies.

Sending Information to Third Parties

Before any confidential information (outside the scope of ZESTIOT.'s regular product offerings) is passed to any third-party organization, authorization shall be received from the Director – Digital Solutions that will include who will contact the third party, who will be contacted, and what information will be shared. Appropriate non-disclosure agreements must be in place with any non-law enforcement agency before information is shared with that agency.

Security of Third-Party Access:

Identification of Risks from Third Party Access

The Director – Digital Solutions will control authorization for types of access to information processing facilities by third parties based upon the reasons for that access.

A risk assessment will be carried out before any third-party access is granted and will consider the reasons for access as well as the necessary controls to be put in place.

Access of third parties to Information Processing facilities will be clearly spelled out in contracts; this access includes the scope of access to physical, logical and network assets.

Security Requirements in Third Party Contracts

The Director – Digital Solutions will control authorization for types of access to information processing facilities and ZESTIOT information by third party contractors.

Any disclosure of confidential information to consultants, contractors, temporary employees, or any other third parties shall be preceded by the receipt of a signed ZESTIOT non-disclosure agreement (NDA).

Access by third party contractors will be specifically agreed upon and documented in contracts.

Arrangements involving third party access to organizational information processing facilities should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with ZESTIOT's security policies and standards. The contract should ensure that there is no misunderstanding between the organization and the third party. ZESTIOT should satisfy themselves as to the indemnity of their supplier. The following terms should be considered for inclusion in the contract:

The general policy on information security.

Asset protection, including:

- Procedures to protect organizational assets, including information and software.
- Procedures to determine whether any compromise of the assets, i.e. loss or modification of data, has occurred.
- Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract.
- Integrity and availability.
- Restrictions on copying and disclosing information.
- A description of each service to be made available.
- The target level of service and unacceptable levels of service.
- Provisions for the transfer of staff where appropriate.
- The respective liabilities of the parties to the agreement.
- Responsibilities with respect to legal matters, i.e. data protection legislation, especially considering different national legal systems. If the contract involves cooperation with organizations in other countries.
- Intellectual property rights (IPR's) and copyright assignment and protection of any collaborative work.
- Access control agreements, covering:

- Permitted access methods, and the control and use of unique identifiers such as user ID's and passwords.
- An authorization process for user access and privileges.
- A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are regarding such use.
- The definition of verifiable performance criteria, their monitoring and reporting.
- The right to monitor, and revoke, user activity.
- The right to audit contractual responsibilities or to have those audits carried out by a third party.
- The establishment of an escalation process for problem resolution, contingency arrangements should also be considered where appropriate.
- Responsibilities regarding hardware and software installation and maintenance.
- A clear reporting structure and agreed reporting format.
- A clear and specified process of change management.
- Any required physical protection controls and mechanisms to ensure those controls are followed.
- User and administrator training in methods, procedures, and security.
- Controls to ensure protection against malicious software
- Arrangements for reporting, notification and investigation of security incidents and security breaches.

Involvement of the third party with subcontractors.

These security requirements must address the confidentiality of ZESTIOT.'s data and the third party's relationships with any ZESTIOT competitor. This is especially important when dealing with engineering partners who work with various companies in the same space as ZESTIOT.

Security Requirements in Outsourcing Contracts

The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks and/or desktop environments should be addressed in a contract agreed between the parties.

The contract should address:

- How the legal requirements are to be met, i.e., data protection legislation.

- What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities.
- How the integrity and confidentiality of the organization's business assets are to be maintained and tested.
- What physical and logical controls will be used to restrict and limit the access to the organization's sensitive business information to authorized users.
- How the availability of services is to be maintained in the event of a disaster.
- What levels of physical security are to be provided for outsourced equipment.
- The right of audit

Asset Classification and Control

ZESTIOT.'s data classification system has been designed to support access to information based on the need to know so that information will be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, ZESTIOT unduly risks loss of member relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

Applicable Information: This data classification policy is applicable to all information in ZESTIOT's possession, including electronic data, printed reports, and backup media.

Consistent Protection: Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, all employees are expected to apply and extend these concepts to fit the needs of day-to-day operations.

Accountability for Assets

To maintain accountability for assets, ZESTIOT will compile a list of all its information assets and establish the relative value and importance of each asset.

This policy requires that all information systems be identified and documented with a program in place to manage assets company-wide. The following will be included in the program:

All assets associated with each information system shall be identified and documented with their classification, owner, and location

All assets shall have an owner and that owner shall be documented

All assets shall be classified based upon their value and importance to the organization and/or to the organization's members.

Classification of security assets will reflect their security protection levels and their handling.

Assets will be categorized into logical categories such as information assets, software assets, physical assets and service assets

Classification Guidelines

Asset classification is the process of assigning value to data in order to organize it according to its sensitivity to loss or disclosure. All information assets shall be classified, using a company-wide asset classification system. All data, regardless of its classification, will be protected from unauthorized alteration; this policy provides guidance on the proper handling of data.

The classification system will allow that classifications of information assets may change over time.

Classifying Information

This policy requires that all information assets be classified and labeled in a manner that allows the asset to be readily identified to determine handling and protection level for that asset.

Care will be taken when interpreting the classification systems from other organizations as their classification systems may have different parameters. Information assets shall be assigned a sensitivity classification by the asset information owner or their nominees, in accordance with the following classification definitions:

Confidential: Sensitive information requiring the highest degree of protection. Access to this information shall be tightly restricted based on the concept of need-to-know. Disclosure requires the information custodian's approval and, in the case of third parties, a signed confidentiality agreement. If this information were to be compromised, there could be serious negative financial, legal, or reputational impacts to ZESTIOT or ZESTIOT.'s members. Examples include member share information, employee performance reviews and salary details.

Internal: Information that is related to ZESTIOT business operations, but not available for public consumption. This information shall only be disclosed to third parties if a confidentiality agreement has been signed. Disclosure is not expected to cause serious harm to ZESTIOT, and access is provided freely to all employees. Examples include policies and standards, operational procedures, etc.

Public: Information that requires no special protection or rules of use. This information is suitable for public dissemination. Examples include press releases, marketing brochures, etc.

The Director – Digital Solutions is responsible for maintaining the policy and ensuring the infrastructure exists to support this policy.

Date of Issue	Standard Operating Procedure Subject:	
31st March 2023	Information Security Policy	2022/SOP/001/01

Handling and Protection Rules

Each asset classification shall have handling and protection rules. These rules must cover any media the assets may reside in at any time

All computer-resident confidential information shall be protected via access controls to ensure that it is not improperly disclosed, modified, deleted or otherwise rendered unavailable.

Employees are prohibited from recording confidential information with tape recorders, digital/analog recording devices, etc., without the consent of technology team. This includes the use of camera equipment (of any kind) in any lab.

Unless it has specifically been designated as "Public", or "Internal", all ZESTIOT internal information shall be assumed to be confidential and shall be protected from disclosure to unauthorized third parties.

No confidential information of ZESTIOT or of any third party shall be disclosed to the public or any unauthorized third party without the prior approval of ZESTIOT's Legal and communication team's approval.

Access to every office, computer room, laboratory, and work area containing confidential information shall be restricted, and employees shall take all reasonable steps to protect confidential information under their control from inadvertent disclosure.

Handling and protection rules must include all parts of an asset's lifecycle, from creation/installation through use and finally to destruction/disposal. Sensitive information or systems must be appropriately disposed of when no longer needed.

Information Labeling and Handling

It is important that an appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by ZESTIOT. These procedures must cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information processing activity.

- Copying
- Storage
- Transmission by post, fax, and electronic mail
- Destruction
- System outputs containing confidential information shall carry an appropriate classification label

The labeling should reflect the classification according to the rules established in Items for consideration include printed reports, screen displays, recorded media (tapes, disks, CD's, cassettes), and electronic messages and file transfers.

Physical labels are generally the most appropriate forms of labeling. However, some information assets, such as documents in electronic form, cannot be physically labeled and electronic means of labeling need to be used.

All printed, handwritten, or other paper manifestations of confidential information shall have a clear sensitivity label on the bottom right hand corner of each page or a watermark that indicates the sensitivity classification.

Information Retention

Information shall not be retained any longer than the business requires it to be retained. This reduces the window of time that data can potentially be available for misuse. Controls should be implemented to delete data that exceeds required retention time.

Electronic member data shall be retained for up to five (5) years.

3.0 PERSONNEL SECURITY

3.1 Security in Job Definition and Resourcing

3.1.1 Personnel Screening Policy

ZESTIOT conducts background checks to ensure the safety of existing employees and to ensure that the employees we hire possess the highest possible level of integrity and business ethics.

The purpose of this policy is to assure that information assets are protected from personnel that may not be trustworthy of the responsibilities associated with security protection and handling.

All screening and supervision shall be in accordance with appropriate legislation in the relevant jurisdiction. The Legal head will publish guidelines for relevant legislation.

3.1.2 Types of Background Checks

ZESTIOT requests the following types of background checks for all positions:

- Employment verification
- Criminal Records Search (up to 7 years)
- Education Verification (for highest level only)

ZESTIOT requests a Credit Check for all Member Service (i.e. access to member data), Finance Management and Executive-level positions.

ZESTIOT requests a Motor Vehicle Check for any position in which use of a company vehicle is possible. This does not include use of a private vehicle for company business.

3.1.2.1 When to Request a Background Check

If the hiring manager is considering making an offer to a candidate, a background check should be requested any time after the first Interview.

3.1.2.2 Who Decides if a Candidate Passes the Background Check?

The hiring manager and ZESTIOT Security Officer will make the determinations as to whether a candidate passes the ZESTIOT guidelines for the background check.

3.1.2.3 Who Requires a Background Check?

All new employees of ZESTIOT require the successful completion of a background check prior to beginning their first day of work at ZESTIOT.

3.1.2.4 Confidentiality Agreements

ZESTIOT expects that information disclosed to ZESTIOT employees will be treated with the appropriate level of confidentiality. Except as required by law, information concerning the Company's business is not to be discussed with competitors, outsiders, or the media. Employees are prohibited from forwarding e-mails containing information on the Company's business to anyone outside of the Company or otherwise transmitting Company-confidential information outside of the Company, whether over the Internet or otherwise. Failure to honor this confidentiality requirement may result in disciplinary action, up to and including, termination of employment.

In the course of employee's work, they will have access to ZESTIOT's confidential and/or proprietary information, including information concerning members (i.e. share/account numbers) and suppliers, as well as fellow employees. It is imperative that no employees disclose such information in any inappropriate ways, and that such information be used only in the performance of regular job duties.

ZESTIOT requires confidentiality or non-disclosure agreements from all employees and third-party staff not otherwise covered by third party contracts before access to sensitive information will be allowed.

This policy requires that staff sign a confidentiality or non-disclosure agreements (unless otherwise contractually bound) prior to being granted access to any sensitive information or systems.

Agreements will be reviewed with the staff member when there is any change to the employment or contract, or prior to leaving the organization.

The Legal Officer will provide the agreements the employees and be responsible for maintaining all agreements in use by ZESTIOT. The following ZESTIOT-approved confidentiality agreements will be used, as appropriate to the circumstance:

Employee Confidential Information, Inventions, No solicitation and Noncompetition Agreement

Only employees who are Assistant manager or above shall sign non-disclosure agreements or any type of contract, such as warranty and Terms and Conditions. All requests for information about ZESTIOT and its business shall be referred to ZESTIOT.'s Legal and procurement department.

3.1.2.5 Terms and Conditions of Employment

ZESTIOT will state the employee's roles and responsibilities for information security in the terms and conditions of employment.

The purpose of this policy is making clear to all employees their responsibilities for maintaining and promoting security within the organization during and subsequent to their employments as well as the sanctions for not doing so.

Human Resources will provide each new employee with the employee's responsibilities for Information Security in the Employee Handbook. This handbook will contain information on Information Security policies, acceptable use, and ethics (direct information or instructions to obtain and read referenced policies).

The employee's manager will provide the employee specific responsibilities that are particular to the specific position.

3.2 User Training

3.2.1 Information Security Education and Training

All employees will be appropriately trained on the organization's Information Security policies and kept up to date on any additions or changes to the policies. Training is mandatory prior to receiving access to information or services.

The Human Resources department is responsible for initial training and education on the organization's security policies during the employee orientation process. Employees should have recurring annual refresher training on current threats, as well as material changes to policy. This training may be conducted by annual refresher seminars or continual reminders (such as posters, e-mail or intranet newsletters, etc.)

When employees sign acknowledgements for complying with policy, these acknowledgements should include acknowledgement of initial training.

The Director – Digital Solutions will be responsible for the on-going policy education and training policy.

3.3 Responding to Security Incidents and Malfunctions

3.3.1 Reporting Security Incidents

ZESTIOT will educate employees on and establish formal reporting and feedback procedures and incidence response procedures for all security incidents. In this way, ZESTIOT will react to all security incidents

immediately and providing all employees with the information necessary to assist the organization is doing so immediately.

All suspected policy violations, system intrusions, virus or malware impact and other conditions that might jeopardize ZESTIOT information or ZESTIOT information systems shall be immediately reported to Director – Digital Solutions.

If an employee learns that ZESTIOT confidential information has been lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the employee shall immediately notify the owner of the information or Director – Digital Solutions.

The Director – Digital Solutions will inform employees how to report possible incidents by providing information to Human Resources to be included in the initial training material.

Incidents may be used in on-going security awareness training to illustrate policy or procedures

Incidents will be reviewed for the purposes of learning how they can be avoided in the future.

3.3.2 Reporting Security Weaknesses

ZESTIOT requires all users to immediately report suspected security weaknesses in, or threats to, systems or services to management or service providers. These weaknesses should only be reported if discovered by the user, as the Director – Digital Solutions will maintain a watch for vendor and forum notifications of new vulnerabilities.

Only users authorized by the Director – Digital Solutions may test systems for suspected security weaknesses. Any unauthorized testing by users shall be considered misuse of the system and be subject to disciplinary measures.

3.3.3 Learning from Incidents

Incidents and malfunctions will be reviewed during the security review process. Analysis of incidents and malfunctions will be done to determine new controls that can be established to prevent future incidents

3.3.4 Disciplinary Process

In support of the Information Security Program, ZESTIOT will establish a formal disciplinary process for those who violate the organization's security policies and procedures.

Disciplinary processes shall be documented by Human Resources and given to all employees and applicable third parties. Discipline for violating security policy or causing a security breach will be as appropriate, up to and including termination or possible criminal/civil charges.

If an employee is suspected of a breach of security, management shall be informed and Director – Digital Solutions, together with the manager of the person suspected, shall begin the investigation.

4.0 PHYSICAL AND ENVIRONMENTAL SECURITY

4.1 Secure Areas

Physical Security Controls

Physical entry controls will be used to protect all secure areas. These controls will be designed to prevent unauthorized access, damage or interference to the business processes that take place within the area. Physical security controls apply to any ZESTIOT owned or controlled facility, including temporary locations.

Site Risk Assessment

A risk assessment of secure areas to determine the type and strength of the physical entry control that is appropriate and prudent. The security controls for an area should be commensurate with the value and classification of the information resources contained. This risk assessment must also consider the physical surroundings of the site. Finally, physical security requirements should include items such as fire suppression, plumbing, and electrical wiring as these may not always be mandated by local authorities.

Site risk assessments must be conducted for any sites where ZESTIOT will be sharing facilities with any outside organization. This may be sharing a building (where physical access is common to all, but network access is specific to each organization) or where ZESTIOT is sharing a suite (where physical and network access is common to all) with others. Specific security requirements must be determined for these situations, based on the arrangements.

Where sites are deficient in physical security controls (such as leased sites where the owner will not allow modification to the structure, or shared sites with business partners), additional network security controls are warranted to protect the rest of the corporate network. In addition, the levels of sensitivity of information that can be processed or stored there may be restricted.

Restricted Access to Sites

Access to sensitive information and information processing facilities will be restricted to authorized persons only. Authentication controls will be used to authorize and validate entry. A log of all that enter will be maintained by the site manager as appropriate for the sensitivity of the information resources. Physical barriers (i.e., doors) must be of enough strength and construction to deter entry, based on the results of the risk assessment.

Controls to restrict access to facilities will be determined on a case-by-case basis. These controls will ensure that unauthorized persons do not have easy physical access to the facilities, and such access is detected, and the appropriate personnel notified if a breach occurs. The Director – Digital Solutions will publish standards for access controls and other physical security measurements commensurate with the classification levels of data present and the information protection requirements.

Access rights will be given on a least-privilege basis and will be as granular as necessary to appropriately protect various classifications of information or facilities. Access rights to secure areas will be reviewed by the site manager periodically and updated where necessary.

4.1.1 Visitor Procedures

All visitors to secured areas will be supervised and only allowed in for authorized purposes. A visitors' log will be in place at all secure areas that records date and time of entry and exist times. All visitors will be given both security instructions and emergency procedures (if applicable).

Employees will challenge unfamiliar people who are unescorted or not showing visible identification.

Contractors, service vendors, suppliers, material men, etc., shall be advised of the building rules and regulations concerning their proper conduct within ZESTIOT's property. They will be required to sign acknowledgement of the BUILDING RULES AND REGULATIONS prior to beginning work.

4.1.2 Third Party Physical Security at ZESTIOT Facilities

Special situations may arise where third parties will have personnel and devices at ZESTIOT facilities on a full-time basis. These third parties must only be allowed full time access if they serve to augment the core capability or flow of ZESTIOT.'s business. Special care should be taken to limit access of third-party personnel to only their work areas as much as possible.

4.1.3 Control of Physical Security Controls

Access to the mechanisms that control physical access to secure sites must be done on the least-privilege basis. This includes access to badge enabling systems, door lock keys, or any other physical access control systems. Master badges or keys must be restricted to very few individuals per site or system. Wherever possible, control of these systems must reside with the local Information Security or Physical Security management.

4.1.4 Securing Offices, Rooms, and Facilities

All offices, rooms and facilities that contain other than public information resources will be protected accordingly to prevent unauthorized access, damage or interference to the business processes.

Site Risk Assessment

A risk assessment of secure areas to determine the type of control that is appropriate and prudent, considering not only personnel risks, but also that of environment, neighborhood, civil unrest, and natural and man-made disasters shall be conducted. Health and safety regulations and concerns will also be examined, and controls incorporated.

Information processing facilities that are managed by third party organizations shall be separated from those that are managed in-house.

Securing Sites when Unoccupied

Rooms in facility that contain sensitive assets will be locked when not in use. Windows and doors will be kept locked and have protection from intrusion or environmental factors. Intrusion alarms will be in place and maintained to the vendors' standards as applicable according to the information protection requirements. Unoccupied areas will be alarmed as required.

Sensitive documents will be locked in file cabinets or other protective furniture that considers the results of the risk analysis.

Additional controls will be implemented for computer and communications rooms or areas. Key facilities will be situated so as they avoid public access. Support functions and equipment will be situated in a way that keeps them away from the public and unauthorized personnel.

Signage and Directory Listings for Secure Sites

The uses of buildings that contain sensitive materials or processing facilities will be unobtrusive and not marked in such a way that gives the public and indication of their purpose or function.

Monitoring of Facilities for Physical Security

Where possible, systems shall monitor the physical security of facilities. Monitoring could include any or all the following technologies, based on the outcome of the physical security risk assessment:

- Closed circuit TV or video cameras
- Glass break sensors
- Door and window opening alarms
- Hold open sensors for doors or windows
- Always-active door alarms for emergency exits and other little used doors
- Above or below ceiling sensors (sites with false ceilings and walls that do not extend from floor to ceiling
- Motion/heat sensors for sensitive working areas
- Security Patrols

Other Site Security Issues

Hazardous or combustible materials shall be stored securely a safe distance from secure facilities. Only necessary bulk supplies shall be stored within secure facilities.

Back-up equipment and media shall be stored off-site and a safe distance from facilities enough that it would not be damaged if the facility is damaged.

5.0 COMMUNICATIONS AND OPERATIONS MANAGEMENT

5.1 Operational Procedures and Responsibilities

5.1.1 Documented Operating Procedures

All standard operating procedures will be formally documented and maintained to ensure the correct and secure management of all information processing facilities.

Formal documented procedures and detail execution instructions will be in place for each job, including:

- Information processing and handling.
- Scheduling requirements including system interdependencies and prioritization.
- Scheduling of earliest start and latest completion times.
- Instructions for error handling, during job execution.
- Instructions for exceptions during job execution.
- Restrictions on the use of system utilities.
- Operational and support contacts for technical difficulties.
- Output instructions for confidential or sensitive output.
- Secure disposal of output from failed jobs.
- System restart and recovery procedures in the event of system failure.
- Housekeeping functions in information processing facilities such as startup and close, equipment maintenance, computer room and mail management and safety; and
- Housekeeping functions in communication facilities such as startup and close, equipment maintenance, computer room and mail management and safety.

Formal authorization from management will be obtained prior to any changes to documentation.

5.1.2 Operational Change Control

Formal management responsibilities and procedures to control all changes to equipment, software or procedures will be established and followed for change, integrating operational and application change control procedures, and logging all changes.

There shall be a formal approval for proposed changes (that could potentially impact the computing environment) that will be developed by the development management team.

Prior to any operational change there shall be a risk assessment that:

- Identifies significant changes;
- Records significant changes;
- Assesses the potential impact of such changes; and
- Procedures and responsibilities for aborting and recovering from unsuccessful changes.

All changes shall be communicated to all relevant persons. The system owner shall manage this process with the assistance of the Chief Information Security Officer.

5.2 System Planning and Acceptance

5.2.1 Capacity Planning

To limit disruption to the network, applications, and business functions, ZESTIOT will monitor system capacity and plan for future capacity needs in sufficient time to procure system resources prudently. This will ensure adequate resources are available and reduce the possibility of system overload.

System owners shall monitor their equipment for current uses and projected capacity.

5.2.1.1 Provisioning of Hardware and Software

IT must be consulted whenever deploying any new systems for adequate provisioning of system hardware and software to take advantage of any contracts or discounts that may be in place. IT will obtain and install the equipment, as appropriate, and then allow access to the appropriate groups for use of the equipment. Provisioning of software requires purchasing of any applicable licenses for use.

5.2.1.2 Management of Network Storage

To allow adequate storage capability to support all users, IT will develop standards and processes for managing online and offline storage capacity. These standards will include types or classes of storage, data backup, protection by classification and any quotas necessary based on the business reasons for storage. Management of storage will incorporate any requirements given in information retention policies

5.2.1.3 System Acceptance

To ensure new systems or applications do not disrupt the network, existing applications, or other systems, a system acceptance process will be defined. This process will document acceptance criteria for new systems prior to acceptance. All systems will be tested prior to acceptance, including a vulnerability assessment or scan prior to being permitted to connect to the ZESTIOT network. This

process will ensure that security controls are in place and that the new system complies with the design and function required.

System owners shall ensure that the equipment capacity requirements are met prior to use of new system.

Managers and users (when applicable) shall inspect major new systems periodically throughout the development to ensure functionality is appropriate and compliant with design requirements.

Prior to the acceptance and use of new systems the following controls shall be documented and in place:

- The system is built according to standard hardware or software builds, published by Technology
- Effective manual contingency procedures are documented (if applicable)
- Error recovery/restart procedures and contingency plans (if applicable)
- Updated business continuity plans (if applicable)
- Compatibility of new system to the security requirements of the organization
- Compatibility of the new system to the existing systems
- Security controls are in place and tested
- Vulnerability scan run against system to verify that patch levels are current and that no unnecessary services are running.

Users shall be adequately trained prior to taking a new system into operational mode.

Operational testing procedures shall be documented and preparation for new system completed prior to acceptance. Systems must meet acceptance criteria, or have formal exceptions authorized, before being connected to the ZESTIOT network.

Note that these requirements do not apply to any system not connected to the ZESTIOT corporate network. This includes stand-alone systems. If these systems are subsequently brought out of that environment and the desire is to connect them to the ZESTIOT network, then these requirements apply once again.

5.2.1.4 Deployment of Network Infrastructure Systems on the Production Network

Network infrastructure systems, such as Domain Controllers, DNS servers, DHCP servers, or other similar systems will not be deployed on the production network except by Technology. If other departments require these services for projects, they must request these services to be deployed by Technology, and these services must be configured to not interfere with the existing

infrastructure of the network. There is no restriction in deploying these services on isolated networks.

5.2.1.5 Third Party Systems on the ZESTIOT Network

If partners or vendors require placement of their devices on the ZESTIOT network, special acceptance criteria must be applied. Third party devices must meet all system acceptance criteria as if they were ZESTIOT systems, in addition to special access to the network. ZESTIOT may not necessarily have physical or administrative control of the systems, so mitigating network controls must be also put in place.

Third party devices must be restricted in the access they may have on the network. This should be implemented using Access Control Lists on the closest network device or other similar technologies. Third party systems should be placed on an 'island' or other segregated network segment allowing only specific data (required by the business) transferred between that network and the rest of the ZESTIOT network.

The placement of such devices must be approved by the Director – Digital Solutions and the Infra Manager before the device may be connected.

5.3 Protection Against Malicious Software

ZESTIOT shall implement procedures, user awareness, and change controls to detect and prevent the introduction of malicious software into the organization's computing environment. This policy will protect the integrity of software and information by promoting procedures and user actions to mitigate the risks of the introduction of malicious software into the organization.

To prevent interrupted service caused by computer viruses for both computers and networks, all personal computer users must always keep current versions of approved virus-screening software enabled on their primary computers.

The organization shall comply with the requirements of software licenses. No unauthorized or illegal software will be used.

All e-mail attachments will be scanned when entering the network or server scanned prior to use. All unauthorized files or amendments will be thoroughly investigated.

Procedures and responsibilities for the use of, training in, reporting on and recovery of virus attacks will be developed and documented. All users will receive training on virus awareness and virus control procedures. Business contingency plans shall include the handling and recovery from virus attacks.

Management will research and actively inform users about information on real (vs. hoax) threats and the procedures for handling each type of attack. The Director – Digital Solutions shall lead this effort.

5.4 Housekeeping

5.4.1 Information Backup

ZESTIOT will regularly back-up adequate copies and generations of all software, documentation and business information and store it off-site. Regular testing will be done to ensure the quality and usability of backed-up resources. The purpose of this policy is to maintain the availability and integrity of information resources in the case of failure or disaster, by retaining up-to-date back-ups that are stored at a distance enough to escape damages that might occur at the main site.

Restoration procedures will be documented and tested to ensure that they are effective and comply with restoration time requirements. Restoration procedures shall be kept with the back-up copies at the remote location.

The back-up site shall implement similar physical and environmental controls as the ones in place at the main site.

Back-up media shall be tested semi-annually to ensure the back-up can be relied upon. Technology shall be responsible for ensuring that back-ups are tested.

Retention schedules will be adhered to for all business information.

Determinations for the permanent archival shall be determined by the Legal Officer and shall be documented and adhered to.

5.4.1.1 PC Data Backup

To protect ZESTIOT.'s information resources from loss or damage, personal computer users are responsible for regularly backing-up the information on their personal computers to their respective network file shares that are assigned to them. These shares are backed up nightly to secure media for disaster recovery purposes.

5.5 Network Management

5.5.1 Network Controls

ZESTIOT shall implement strict controls on the organization's networks to ensure the safeguarding of information and protection of the organization's infrastructure. Controls shall guarantee the security of data in networks and protect the connected services from unauthorized access.

All procedures and responsibilities will be documented.

Network access controls will be observed for networks connected to public networks.

The Director – Digital Solutions will closely coordinate the controls on the organization's networks to assure functional optimization as well as consistency of controls.

5.6 Exchange of Information and Software

5.6.1 Information and Software Exchange Agreements

Formal agreements will be put in place when information and/or software are to be exchanged between organizations. This policy is necessary to prevent loss, misuse or modification to the organization's information by establishing secure agreements that reflect the sensitivity of the business information involved in such and organization to organization exchange.

The organization shall seek guidance from an expert or in-house counsel in the area of intellectual property exchange.

The agreements shall cover:

- Responsibilities for controlling and notifying transmission, dispatch and receipt.
- Procedures for notifying sender, transmission, dispatch and receipt.
- Technical standards for packaging and transmission.
- Courier standards.
- Responsibilities and liabilities in case of loss of data.
- Agreed upon labeling system.
- Agreed upon standards for labeling.
- Legal responsibilities for copyright protection, ownership and data protection.
- Technical standards for reading and recording information and software; and
- Special controls for protecting sensitive items.

Agreements shall be formally enacted when the information to be exchanged is of a non-public classification.

The information owner shall be responsible for assuring that agreements are executed.

5.6.2 Security of Physical Media in Transit

The purpose of this policy is to prevent loss, modification, or issue of data that is being physically transported. The organization will safeguard media or information to commensurate with its data classification.

The Director – Digital Solutions will provide a list of reliable experienced couriers. Only these couriers shall be used unless the authorization of the Director – Digital Solutions is obtained.

All media in transit will be labeled accordingly and packed securely in accordance with the manufacturer's specifications.

Sensitive information shall be protected from unauthorized access or modification by methods that include:

- Locked containers
- Hand delivery
- Tamper evident containers
- Splitting the information into more than one package and more than on route

The System owner will approve the method for each transport of sensitive information.

Audit logs will be kept for each transport of sensitive media (a classification level of non-public) including:

- What was sent
- To whom it was sent
- Who sent it
- Dispatch time
- Arrival time
- Method of transport
- Special protections
- System owner's approval

5.6.3 Security of Electronic Media in Transit

The purpose of this policy is to prevent loss, modification, or issue of data that is being electronically transported (i.e. email, fax, and file transfer). The organization will safeguard media or information to commensurate with its data classification.

Sensitive information shall be protected from unauthorized access or modification by methods that include:

- Use of digital signature and encryption (see 7.3.3).
- Use of secure use of facsimile equipment (see 7.3.3).

The System owner will approve the method for each transport of sensitive information.

Audit logs will be kept for each transport of sensitive media (a classification level of non-public) including:

- What was sent
- To whom it was sent
- Who sent it
- Dispatch time
- Arrival time
- Method of transport
- Special protections
- System owner's approval

5.6.4 Other Forms of Information Exchange

The following policies govern the secure use of voice, facsimile or video equipment to protect the confidentiality and access to information that is communicated through these mediums and to ensure the availability of resources.

ZESTIOT staff shall not reveal sensitive information on the telephone (land or mobile) that can be:

- overheard by others
- when there is a threat of wiretap or other type of potential eavesdropping
- when others at the recipient's end may be eavesdropping
- in public places or in open offices or offices having thin walls

ZESTIOT staff shall not reveal sensitive information on answering machines that are shared, can be accessed by others or could be the wrong voicemail box.

ZESTIOT staff shall not send or receive sensitive or confidential messages on facsimile machines that store messages.

ZESTIOT.'s staff shall check to assure that the phone number that information is being sent to is correct and verify that the information is received.

ZESTIOT.'s staff shall verify recipient's facsimile information with the recipient prior to sending confidential information. The confidential information shall not be sent until the recipient has stated that the information can be sent.

Access to business resources shall be controlled (see 6.0).

5.6.5 Production of SPAM

ZESTIOT business units will take care not to produce Unsolicited Commercial E-mail (otherwise known as SPAM) to be sent out to the Internet. Any commercial e-mail should be specifically targeted to recipients in accordance with applicable laws and regulations. If allowed mass e-mailings will be made, Technology will be consulted to determine the effects of these mailings on systems and the network, and appropriate mitigation efforts will be enacted (such as system, time of day, or network path restrictions).

5.7 Vulnerability Management

Effective vulnerability management can reduce risk to ZESTIOT's computing environment by verifying that systems or network devices are using current patch levels, are not running unnecessary services, and do not have default passwords.

ZESTIOT shall run internal vulnerability scans against any systems containing (or accessing systems that contain) confidential data at least on a quarterly basis.

ZESTIOT shall contract with a trusted third party to run external vulnerability scans against any Internet-facing systems on at least a quarterly basis.

6.0 Access Control

6.1 Business Requirement for Access Control

6.1.1 Access Controls and Need to Know

ZESTIOT will define and document access control rights and rules for each user or group of users. Service providers shall be given clear statements of the business requirements met by these access controls. Access to information and information services will only be given based on business and security requirements.

Access will be given on a need to know basis, based upon the security requirements and business requirements of individual business applications. Access to information shall be provided in a manner that aims to protect the confidentiality and integrity of that information and without compromise to associated information or raw data. Data owners shall review access control rights for users and groups of users on a bi-annual basis to ensure that all access rights are authorized and remain appropriate, and that no unauthorized privileges have been gained

All forums where confidential information may be discussed and where non-ZESTIOT employees are present shall be preceded by a determination that all parties are authorized to receive the information and the appropriate categorization of that information.

Access will be given that is consistent with security levels and classifications, consistent with legislation and contractual obligations for confidentiality.

Access to standard common groups of users will be given standard access profiles.

Access rights in a networked environment will recognize all connection types available.

All users and groups of users shall receive a clear statement as to the access policy and as to the requirements met by these access controls.

Originators of confidential information shall decide who will be permitted to gain access to that information and shall specify the uses for that information.

Administrator access to production systems will be limited to only those with a justified business requirement for such access. Developers and other application personnel will not have access to the underlying operating system on production systems, except in emergencies and then with access only granted for the time necessary. System administrators shall not have access to the applications if possible.

6.1.2 Types of Access Controls

ZESTIOT has established clear access control rules that distinguish between optional, express, discretionary, automatic and those that require approval.

Access rules will specifically differentiate between those rules that are optional or conditional and those that are always to be enforced.

Access rules will be declarative statements such as “access is forbidden unless specifically permitted” instead of “access is generally permitted unless forbidden”

Access rules will differentiate between permissions that are granted by the information system and those permissions that must be granted by an administrator.

Access rules will differentiate between those rules that require approval and those that do not.

Access rules will consider changes in classifications that are automatic and those classification changes that must be initiated by an administrator.

Access rules for each system will be developed in according with the Information Classification guidelines commensurate with the information’s sensitivity.

6.2 User Access Management

6.2.1 User Registration

A formal user registration and deregistration process must be used for gaining access to multi-user systems. This process must protect and maintain the security of access to the organization’s information resources through the complete life cycle of the user.

Access to ZESTIOT confidential information shall be provided only after the authorization of the information owner has been obtained.

Contractors and third-party contracts will contain the rights of access and will contain sanctions if unauthorized attempts at access are made.

Service providers shall be made aware of policy not to provide access to users until specific authorization has been given.

Each person accessing an ZESTIOT multi-user based information system shall utilize a unique ZESTIOT-assigned User ID and a private password. User IDs shall not be shared among two or more users.

System owners and/or management shall grant access rights. Formal records of all access rights for each system shall be maintained.

Access rights shall immediately be removed or modified when a user leaves the organization or changes jobs.

Technology will periodically check for redundant IDs and ensuring that redundant IDs are not issued in excess of that required (i.e., administrators may have a privileged and a non-privileged account on the same system, but an average user should not have two different non-privileged accounts on the same system without a valid business reason).

6.2.2 Privilege Management

User rights shall be granted using the least-privilege methodology, based on business need and security requirements.

All privileges shall be granted only with formal authorization. This authorization shall be accomplished along with User ID authorization, according to IT guidelines. All privileges that are granted will be documented. No privileges shall be granted until authorization is complete.

Elevated privileges (Administrator or root, etc.) should be assigned to a different user ID than that used for normal business use. Administrators should only use their elevated privilege accounts when conducting activities that require them. Elevated privileges must only be assigned to dedicated systems administrators and not normal users.

Wherever possible system routines should be developed and used instead of privileges.

6.2.3 User Password Management

A user's account and password are the primary means of verifying a user's identity. The allocation of passwords will be a formal management process.

Users will sign a statement in their terms and conditions of employment that they will keep their personal or group passwords confidential. This may be done as part of the overall acceptance of policies.

Users will be responsible for the secure storage of their passwords.

Users will be granted initial temporary passwords and will be forced to change them immediately. Initial passwords will be unique for each user. Temporary passwords will only be granted with positive identification of the user.

Passwords will be given in a secure manner (i.e. not in a plain text e-mail)**.**

6.2.4 Review of User Access Rights

Users' access rights will be reviewed at regular intervals. Managers will review their employee's rights to ensure they are consistent with their present job function. Technology will review user rights to ensure that elevated privileges have not been granted out without authorization, and that accounts that have not been used recently or belong to terminated employees are deactivated or purged.

User access rights shall be reviewed at least every 6 months. Privileged access rights shall be reviewed every 3 months to ensure that all are authorized and remain appropriate and that no unauthorized privileges have been gained.

6.3 User Responsibilities

6.3.1 Password Use

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of ZESTIOT.'s entire corporate network. As such, all ZESTIOT employees (including contractors and vendors with access to ZESTIOT systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

6.3.1.1 User Password Rules

All users will keep their passwords confidential and store them securely (i.e. not on the computer and not on paper unless they can be protected).

Users will be made aware of good security practices and the requirement to use good security practices with their passwords.

All passwords are to be treated as confidential ZESTIOT information. They should not be shared with anyone, including administrative assistants.

Password requirements:

- If an account or password is suspected to have been compromised, report the incident to Information Security and change all passwords.
- Regular passwords shall be changed at least every 3 months (90 days).
- Privileged passwords shall be changed every 90 days.
- Shared privilege passwords (i.e. for "root", "administrator", etc. should be changed every 90 days or whenever someone with administrator-level access leaves the firm.
- Passwords cannot be re-used for a minimum of 12 months or 10 passwords.
- Temporary passwords will be changed at first log-on.

- Systems shall be configured to lock user accounts in the event of 5 consecutive unsuccessful login attempts. System Administrators may reset locked accounts; otherwise the minimum account lockout duration shall be 24 hours.

Passwords will not be stored on a computer or used in a macro for sign-on.

Do not use the "Remember Password" feature of applications.

Passwords may not be inserted into e-mail messages or other forms of electronic communication.

Passwords should not be written down or stored unencrypted on ANY computer (including PDA's)

6.3.1.2 System Password Rules

System accounts (i.e., non-interactive accounts for applications or systems) must use passwords that meet or exceed the password composition requirements.

System-level passwords must be changed at least once every 90 days. This includes shared secret keys for encryption of connections.

Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (i.e., SNMPv3).

6.3.1.3 Password Composition

All user-level and system-level passwords must conform to the requirement described below.

Passwords will be at least 8 non-sequential characters long.

Passwords will be composed of alpha-numeric characters.

Passwords will contain at least 3 of the 4 characteristics below:

- alphabet character
- upper case letter
- number
- non alpha-numeric character

6.3.2 Unattended User Equipment

Users shall protect ZESTIOT.'s information resources from unauthorized access by protecting unattended equipment:

- Users will terminate active sessions when finished (or unattended) or secure by appropriate locking functions.
- Users will log off multi-user systems when finished.
- Users will log off or lock terminals when unattended.
- PCs or terminals shall be locked (i.e. by a key or password) when not in use.
- A password-protected screen saver will be automatically invoked after 15 minutes of inactivity.

6.4 Network Access Control

6.4.1 Policy on Use of Network Services

Users shall only have access where there is a specific business requirement and the access has been specifically authorized. Users will be granted specific access to networks that they are permitted to access. Users may not access networks that they are not given specific authorization to access.

Information Security shall provide users with the rules, policies and procedures for accessing network connections and network services.

Third parties that must deploy non-ZESTIOT controlled systems must be specifically approved by the Director – Digital Solutions and must meet the third-party provisions of section.

6.4.2 User Authentication for External Connections

All remote users will be authenticated before they are permitted to access information resources. Users will be given remote access only when their job function requires it. Any non-employee who receives approval for remote access must be to access to specific systems only.

The system owners, in coordination with the Director – Digital Solutions shall select from the following options, based upon the results of the risk assessment:

- Cryptography
- Hardware tokens
- Challenge/response protocol
- Dedicated private lines
- Network user address checking
- Dial-back procedures and controls (without call forwarding)

All procedures and controls shall be thoroughly tested prior to use.

6.4.3 Remote Diagnostic Port Protection

Remote diagnostic ports, usually in the form of vendor modems attached to systems, must be protected from unauthorized use. Diagnostic ports shall not be connected when not in use. The Director – Digital Solutions must approve any requests for a vendor or third party to access a device through a remote port. The vendor must be fully authenticated before access is granted.

Information Security/Technology must review the system after the vendor has accessed it to ensure no unauthorized activities were performed on the system.

6.4.4 Segregation in Networks

6.4.4.1 External Segregation

Network Controls must segregate groups of information services, users and information systems when interconnecting networks to partners or other third parties.

A risk assessment must be performed to determine the necessary controls prior to allowing access of the organization' networks by new partners or third parties, and the Director – Digital Solutions must approve of any such connections.

Network segregation controls will be selected based on the risk assessment; cost and the impact of incorporating suitable routing and gateway technology. External connections must terminate in some form of controlled network (DMZ or similar) and must be subject to security controls. There shall be no direct connection between the ZESTIOT corporate (internal) network and any third party.

6.4.4.2 Internal Segregation

Based on site risk assessments, internal segregation of sites or networks within sites may be warranted. Development and testing networks/systems must be segregated from the rest of the internal network (either completely or through a firewall/proxy arrangement) to prevent malfunctions in software from impacting the rest of the network. In addition, certain locations (such as locations where there is civil unrest or rampant crime) must be adequately segregated from the rest of the network to ensure the security of corporate information assets.

Confidential information shall be consolidated and isolated on dedicated access servers, active storage and inactive storage (such as tape media) whenever possible.

6.4.4.3 Segregation of Development and Production Environments

ZESTIOT will separate development and production environments to prevent unfinished or malfunctioning software from affecting the business network. Only Technology-approved systems

will be connected to production environments, and only after the systems have fulfilled acceptance criteria.

6.4.5 Network Connection Control

Highly sensitive systems will have network access controls (i.e., firewalls or Access Control Lists) in place to prevent unauthorized connections from inside, or outside, ZESTIOT. This is in addition to any application or system access controls. Restrictions will be consistent with the organization's access control policy.

Network controls shall be configured to allow only network traffic required by the business to enter or leave the ZESTIOT network. The Director – Digital Solutions shall work with management to determine those business requirements. These controls shall include:

- Ingress and egress filtering on border devices
- Firewall/Access Control List configuration that is host and port specific.

An annual risk assessment will be performed to establish which systems and/or applications should be protected.

6.4.6 Wireless Network Policy for ZESTIOT Facilities

This policy prohibits access to ZESTIOT Corporation networks via wireless communication mechanisms.

This policy covers all wireless data communication devices (i.e., personal computers, cellular phones, PDAs, etc.) connected to any of ZESTIOT Corporation's internal networks.

This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to ZESTIOT Corporation's networks do not fall under the purview of this policy.

6.5 Operating System Access Control

6.5.1 User Identification and Authentication

All users shall be identified and authenticated with the minimum of a unique identification and a password before access to operating systems is granted. This will minimize the opportunity for unauthorized access to information resources at the operating system level by providing a means of user authentication. If access to the operating system is not necessary, such as when the user has access to an application (only) running on the system, then operating system access must not be given to the user.

If operating system access is necessary, such access will abide by the following rules:

- All users shall have a unique user account
- All users shall have a unique password
- Users' passwords will give no indication to their privilege level

Additional authentication technique(s) will be used in combination with user IDs to provide further security in authentication including:

- Passwords
- Cryptographic and authentication protocols
- Memory tokens or smart cards
- Biometrics

6.5.1.1 Password Program

All passwords for systems and applications must be individual, effective, and of enough quality to deter compromise. Systems and applications must be configured to programmatically enforce these rules if available. In the absence of programmatic enforcement, the user will be responsible for enforcing these rules themselves.

6.5.1.2 System Password Rules

Default passwords will be changed as soon as a new application is installed.

Systems must automatically expire passwords on the anniversary of the creation of the password. Expiration may lead to disabling of the account or forcing a password change (depending on the software implementation).

Application developers must ensure their programs contain the following security precautions. Applications:

- should require confirmation during selection to avoid input errors
- should support authentication of individual users, not groups
- should not store passwords in clear text or in any easily reversible form
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password
- should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible
- should not be displayed when entered
- should keep password files separate from application system data

6.5.2 User Account Review/Audit

All user accounts shall be reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist. User/group roles and access rights shall be reviewed on a regular basis to ensure that no user or group has excessive privileges.

6.5.3 Use of System Utilities

Access to system utilities for non-administrators should be restricted to minimize the opportunity for unauthorized access to or modification to information resources.

All unnecessary system utilities shall be removed from server systems. Unnecessary system utilities should be removed from desktop/laptop systems as appropriate.

6.6 Application Access Control

6.6.1 Information Access Restriction

To safeguard applications, ZESTIOT will restrict business application system access information on a need-to-know basis.

Menus and documentation shall be edited so the users only view data or menus that they are authorized to view.

Users' rights shall be based on a Least-Privileged basis, so that they limited to only those functions to which they are authorized (i.e. read, write, delete, and execute). User's rights shall be reviewed on a periodic basis to ensure that no user or group has excessive privileges.

Outputs available to users are limited to those to which they are authorized.

Sensitive outputs shall be controlled and limited to specific terminals and/or printers. Sensitive outputs must be controlled and limited to specific users who have a valid business need.

Periodic reviews will be performed to ensure that outputs of sensitive information are required by the business. Any extraneous output of sensitive information will be removed.

6.7 Monitoring System Access and Use

6.7.1 Event Logging

ZESTIOT will log all security-relevant events or exceptions.

Technology will be responsible for maintaining event logs.

Event logs will be retained for at least one year with at least 3 months of on-line retention.

The Director – Digital Solutions will monitor event logs at periodic intervals, not to exceed weekly. Automated log analysis and alerting will suffice for this provision.

Event logs will contain:

- User IDs used in logons
- Dates and times for logon and logoff for each user
- Terminal identity (system name and network address)
- Successful and rejected access attempts
- Successful or rejected data access attempts
- Any access to Member data (Account numbers)

6.7.2 Monitoring System Use

ZESTIOT will monitor the use of information processing facilities to detect unauthorized activities and ensure that users are only performing the functions and gaining access to information to which they are authorized.

Each facility shall perform a risk assessment to determine the level of monitoring required.

6.7.2.1 Monitored Items

Areas eligible for monitoring include:

- Authorized access:
  - ✓ User IDs
  - ✓ Date and time of key events
  - ✓ Types of events
  - ✓ Files accessed
  - ✓ Programs and utilities used
- Privileged operations:
  - ✓ Use of supervisor accounts

- ✓ Use of other privileged accounts (i.e. administrator)
- ✓ System start-up and stop
- ✓ Devise attachment and removal

- Unauthorized attempts:
  - ✓ Failed attempts for access
  - ✓ Access policy violations and notifications for network gateways and firewalls
  - ✓ Alerts from proprietary intrusion detection systems
- System alerts or failures:
  - ✓ Console alerts or messages
  - ✓ System log exceptions
  - ✓ Network management alarms
- All access to Member data, including root/administration access

Monitoring results shall be retained in accordance with retention schedules for potential evidence.

6.7.2.2 Review of Monitored Information

IT and the Director – Digital Solutions will regularly review the results of the monitoring of information processing facilities to detect deviations from the organizations' access policy and to improve and discipline those that deviate.

The factors that determine the frequency of review include:

- ➢ Value, criticality or sensitivity of the information or application involved;
- ➢ Experience of infiltration or misuse; and
- ➢ Extent of interconnections.

Those who violate policies shall be disciplined.

Incidents shall be reviewed, and controls put in place to stop future occurrences.

6.7.2.3 Protection of Monitored Information

Event and security logs must be protected in order to assure their accuracy and to protect them against tampering or misuse.

All original logs must be kept unaltered. Extracted log events shall be kept separately from the original logs.

The review of logs will be segregated from those whose actions are logged.

Controls shall be put in place that prevent and monitor:

- attempts to de-activate logs
- attempts to alter message types that are recorded
- attempts to edit or delete log files
- the log file becoming exhausted and either overwriting itself or failing to record events

The System owners shall be responsible for the reviewing of their system logs.

The Director – Digital Solutions shall audit these reviews.

6.7.3 Clock Synchronization

ZESTIOT will use a common method to ensure that all system clocks are synchronized. This will ensure the accuracy of the audit logs and protect the integrity and credibility of any logs that might need to be used as future evidence.

All computers with real-time clocks shall be set on one time standard (local standard time) that is used within the entirety of the organization.

6.7.4 E-Mail, Voicemail, and Internet Access Monitoring

ZESTIOT.'s e-mail, voice-mail and Internet access systems are to be used primarily for ZESTIOT business. ZESTIOT reserves the right to access e-mail or voice-mail systems at any time with or without advance notice or consent of the employee. Such access may occur before, during or after working hours by any manager or security personnel designated by ZESTIOT.

Employees should not have an expectation of privacy in their voicemail or e-mail messages, or in computers or computer storage devices. ZESTIOT also reserves the right to monitor all Internet access. While ZESTIOT recognizes that accidental access to undesirable sites is unavoidable, prolonged or repeated access to undesirable sites will be construed as intentional violation of ZESTIOT.'s policy and may result in disciplinary action up to and including termination.

All Internet data that is composed, transmitted, or received via ZESTIOT's computer communications systems is part of ZESTIOT's official records and, as such, may be subject to disclosure to third parties.

Employees should always ensure that the business information contained in Internet transmissions is accurate, appropriate, ethical, and lawful.

6.8 Mobile Computing and Teleworking

6.8.1 Mobile Computing

ZESTIOT institutes the following policies to ensure that business information is not compromised by use of such devices as notebooks, laptops, PDA's, and mobile telephones in an unprotected environment and to provide users with controls for and awareness of the potential risks.

A risk assessment will be performed on the potential threats associated with the various forms of mobile computing for new devices (other than those listed above) that become available.

The risk assessment will consider the following issues:

- Physical protection of the device (i.e. locking away, carrying on airplanes)
- Access control (see 6.1),
- The use of cryptographic techniques (see 7.3),
- Back-up schedules, procedures and media protection (see 5.4),
- Protection from viruses and malicious software (see 5.3),
- Network connections (see 6.4),
- Use of networking facilities in public places.

Users of mobile computing devices will be required to sign a statement of their understanding and compliance. This statement should be included in the policy acceptance letter signed during orientation.

6.8.1.1 Physical Protection of Mobile Devices

Users must reasonably ensure mobile devices are always physically secure if they contain ZESTIOT sensitive data. Examples of physically securing devices include:

- Mobile devices should never be left visible and should never be left in the trunk or other storage location overnight.
- Mobile devices should always be carried onboard aircraft and not put in checked luggage

- Mobile devices should not be left at tables in public places (i.e. restaurants) if they will be out of sight

6.8.1.2 Access Control Requirements

If a mobile device contains other than public ZESTIOT data, it must have some form of access control to access this information. If access to the device is not controllable, access to the data must be controlled.

6.8.1.3 Use of Encryption

If a mobile device contains sensitive ZESTIOT data, it must be encrypted on the storage drive. Encryption may be on a file-by-file basis, or on a volume-by-volume basis.

6.8.1.4 Information Backup

Users are strongly encouraged to back up their ZESTIOT data stored on mobile devices. Backup may be done when connected to the ZESTIOT network (file shares and other backup facilities) or may be backed up to removable media. If backed up to removable media, this media must be physically protected, or the data must be encrypted.

6.8.1.5 Protection from Viruses/Malicious Software

If capable, mobile devices must run anti-virus software with current updates/definitions. All laptops must use ZESTIOT-approved anti-virus software.

6.8.1.6 Connecting to the ZESTIOT Network at ZESTIOT facilities

Users may only connect mobile devices that have been authorized by the Director – Digital Solutions to the ZESTIOT network at ZESTIOT facilities. These devices must have current anti-virus software running and the user must be reasonably sure no other malicious software is operating on the laptop.

Users may never connect to an outside network through any form of network interface (modem, wireless, second Ethernet card, etc.) while simultaneously connected to the internal ZESTIOT network through their primary network connection. If use of a secondary connection is necessary, the user must first disconnect from the ZESTIOT network before connecting to the outside network. This policy also applies to connections from one security zone within ZESTIOT to another (i.e., connecting to the ZESTIOT corporate network and the network inside an isolated lab at the same time).

Users are encouraged to have Technology or Information Security check their approved mobile devices before connecting to the ZESTIOT network if they have reason to believe they may have encountered any malicious software, whether detected by anti-virus or not.

6.8.1.7 Connecting to the Internal ZESTIOT Network from Public Places

Remote connections to the ZESTIOT network may be made by mobile devices at public places under the following provisions. Public places are defined as any place outside an ZESTIOT facility and include, but are not limited to hotels, hot spots at food or drink establishments, airports or train stations, employee's or other people's homes, government or partner facilities.

Users must use an approved personal firewall, and have it running and actively filtering traffic, when connecting to ZESTIOT networks from public places. Users must also have current and active anti-virus software running before connecting. Remote connections will be made through VPN tunnels to safeguard the connection traffic. Connections from home networks may use a gateway firewall in place of the personal firewall, but one or the other must be operational and actively filtering traffic.

6.8.1.8 Wireless Connections (if applicable)

ZESTIOT users must use a personal firewall and anti-virus software (as discussed above) whenever connected to a wireless network, regardless of whether they will connect to the ZESTIOT networks. In addition, the use of WPA or equivalent privacy measures is encouraged where available.

Mobile device users will not enable ad hoc networking or operate any other access point functionality on their wireless adapters while connected to the ZESTIOT network through another connection (Ethernet, modem, etc.).

6.8.2 Telecommuting and Remote Access

The purpose of this policy is to ensure that the organization's information resources are not compromised by those that access them from premises that are not under the control of the organization by requiring authorization, controls and monitoring the telecommuting. Also see 6.8.1 concerning mobile devices.

Users must strictly control and protect the organization's information resources against the possible threats associated with telecommuting. These threats include theft of the remote computing devices and unauthorized access into ZESTIOT's computing facilities.

Revocation of remote access rights shall be immediate as soon as telecommuting ceases.

An annual risk assessment will be performed to review users who have remote access privileges to ensure that their job requires them to use remote access services.

6.8.2.1 Authorization for Remote Access

All telecommuting (work that occurs from a fixed location that is outside of the organization that requires connection to the organization's information resources) shall be authorized by the Chief Information Security Officer.

Authorization Rules:

- All telecommuting will be specifically authorized
- The access to sensitive information shall be specifically authorized
- The storage of sensitive information shall be specifically authorized
- The work performed by the telecommuting shall be specifically authorized

Telecommuting Resources:

- The telecommuting shall have adequate and secure communications equipment
- The teleworker shall be given access to hardware and support and maintenance services
- Communication requirements will be secure and in line with those required by the information to be accessed classification.

6.8.2.2 Applicability of ZESTIOT Policy during Telecommuting

Users are responsible for any security breaches that occur as a result of their negligence in securing their personal remote systems. By using their own equipment, users are accepting responsibility to protect the ZESTIOT information in accordance with policy. ZESTIOT reserves the right to audit and monitor any equipment used to process or store ZESTIOT information resources, regardless of ownership.

Remote Access Methods and Authentication of Connections

Users will employ only ZESTIOT approved remote access methods when connecting to the ZESTIOT network. In addition, users connecting remotely will be authenticated using a two-factor method of authentication before being allowed to connect.

This provision applies equally to the connection to the ZESTIOT network and connections to ZESTIOT information resources within the network. Only approved methods of system remote access will be allowed in accordance with Technology guidance and standards.

All use of non-approved access methods, or approved access methods not utilizing IT approved configurations and settings, will be subject to disciplinary procedures.

Access to the ZESTIOT Networks via remote access is to be controlled using strong authentication

At no time will commercial remote access services (such as GoToMyPC or any desk) be allowed with ZESTIOT networks, systems, or home systems that house or process ZESTIOT information.

6.8.2.3 Remote Management of Systems

Remote management connections will only be made via encrypted connections (SSH, SSL, etc.). Where possible, remote connections must not allow logon via an elevated system account (i.e., root or administrator) directly. Administrators must log on with their user account and then change to the elevated privilege account. This will ensure accountability and logging of unique IDs instead of shared administrative accounts.

6.9 Acceptable Use of ZESTIOT Computer Systems

The purpose of this policy is to outline the acceptable use of computer equipment at ZESTIOT. This will help protect ZESTIOT.'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate use exposes ZESTIOT to risks including virus attacks, compromise of network systems and services, and legal issues. All users are expected to be familiar with and comply with this policy.

All ZESTIOT systems are to be used for business purposes in serving the interests of the company, and of our clients and members during normal operations, although occasional use of ZESTIOT computer systems for personal use is acceptable.

Effective security is a team effort involving the participation and support of every ZESTIOT employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know this policy, and to conduct his/her activities accordingly.

This policy applies to employees, contractors, consultants, temporaries, and other workers at ZESTIOT, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by ZESTIOT.

6.9.1 General Use and Ownership

While ZESTIOT.'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of ZESTIOT. Because of the need to protect ZESTIOT.'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to ZESTIOT

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by

departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

Employee shall exercise due diligence to protect sensitive or confidential data or material. For guidelines on information classification, see Information Classification Policy.

For security and network maintenance purposes, authorized individuals within ZESTIOT may monitor equipment, systems, and network traffic at any time.

6.9.2 Security and Proprietary Information

Employees should take all necessary steps to prevent unauthorized access to this information:

- Authorized users are responsible for the security of their passwords and accounts. Users must keep their passwords secure and accounts should not be shared.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
- Postings by employees from an ZESTIOT email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ZESTIOT unless posting is in the course of business duties.
- All applicable hosts used by the employee that are connected to the ZESTIOT network, whether owned by the employee or ZESTIOT, shall continually execute approved virus-scanning software with a current virus database (unless overridden by departmental or group policy).
- Employees must use extreme caution when opening e-mail attachments received, especially from unknown senders, as these attachments may contain viruses, e-mail bombs, or Trojan horse code.

6.9.3 Unacceptable Use

The following activities are generally prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of ZESTIOT authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing ZESTIOT owned resources.

The lists below are by no means exhaustive, but provide a framework of strictly prohibited activities:

6.9.3.1 System, Network, and Internet Activities

Private use of the Internet may be permitted (departmental control) within reasonable limits, provided that the Web sites accessed are not unlawful or inappropriate to a well-controlled working environment (e.g. pornography, gambling or drug-related sites).

The Internet must not be used to violate intellectual property rights of any party. Intellectual property includes copyrights, trademarks, patents, trade secrets, publicity and privacy rights. Employees are prohibited from interfering with or attempting to disable anti-piracy mechanisms or other standard technical measures used by copyright owners to protect or identify their work.

Accessing resources other than web sites on the Internet from ZESTIOT premises is reserved to the authorized users of the target systems, must be limited to legitimate purposes and must comply with local legislation. Attacking in any way, as well as scanning, probing or penetrating, computer systems or networks on the Internet is strictly prohibited. All employees will be made aware that all Internet access may be screened, logged and monitored, in accordance with local legislation.

ZESTIOT reserves the right to block access to Internet sites considered inappropriate. Deliberate attempts to access such sites will result in disciplinary action.

The download of electronic files from the Internet by employees is prohibited unless as a necessary part of their work and must be subject to virus checking on the local workstation.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ZESTIOT or the end user does not have an active license is strictly prohibited.

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.

Employees shall not reveal ZESTIOT member/share account passwords to others or allow use of their accounts by others. This includes family and other household members.

Employees may not use an ZESTIOT computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

It is not permissible to make fraudulent offers of products, items, or services originating from any ZESTIOT account.

Employees shall not attempt to access data for which they have not been granted access, unless they have been granted permission to test security controls of a system or application (i.e. these duties are within the scope of regular duties).

It is prohibited to execute any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.

It is prohibited to circumvent user authentication or security of any host, network or account.

It is prohibited to provide unauthorized information about, or lists of, ZESTIOT employees to parties outside ZESTIOT.

6.9.3.2 Email and Communications Activities

- The use of unapproved instant messaging systems (e. g. AOL Instant Messenger, ICQ) is not permitted.
- Personal, non-business user is permissible to extent that it does not consume significant resources, and that it does not pre-empt any business activity
- E-mail, including attachments must be classified according to the policy, based on the sensitivity of the information contained. Therefore, e-mail has to be secured to an extent commensurate with this classification. Procedures for the correct labeling and the classification of e-mails are defined in the Information Asset Classification Guideline.
- Employees shall not send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- It is prohibited to participate in any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information is prohibited.
- Employees shall not use ZESTIOT email or computing resources to participate in the creation of or the forwarding of "chain letters", "Ponzi", or other "pyramid" schemes of any type.

6.9.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 SYSTEMS DEVELOPMENT AND MAINTENANCE

7.1 Security Requirements of Systems

7.1.1 Security Requirements Analysis and Specification

The purpose of this policy is to ensure that all new systems comply with the organization's security requirements. Security approval shall be required for all key project phases (i.e. concept, requirements, testing). All new or upgraded systems must have their security requirements documented.

A risk assessment will be performed to evaluate the security requirements for new systems or upgrades.

The system owner, in conjunction with the Chief Information Security Officer, will specify the security requirements of all new implementations prior to their final approval.

- The controls and requirements will reflect the sensitivity and business value of the information assets involved.
- Independent consultants will be brought in to assist in evaluations if deemed necessary.
- Vulnerability scans and/or penetration tests will be run against systems to ensure security controls are in place, patch levels are current, and unnecessary services are not running.

7.2 Security in Application Systems

7.2.1 Input Data validation

All applications will validate input data before storing or processing. This will ensure that the data input to systems is correct and appropriate, therefore protecting the integrity of the organization's information systems.

Checks shall be applied to all standing data inputs (i.e. names, addresses, credit limits, and tax rates).

Checks shall be applied to parameter tables (i.e. sales pricing, currency conversion rates, tax rates).

Dual input or other input checks shall be used to detect:

- Out of range values
- Invalid characters in data fields
- Missing or incomplete data
- Exceeding upper or lower data volume limits
- Unauthorized or inconsistent data control

There shall be procedures for testing the plausibility of data inputs.

A periodic review of the content of data in key fields will be done to confirm validity and integrity of data. Procedures shall be put in place to respond to validation errors.

All users shall be trained on their responsibilities involved with input as well as how to respond to input validation errors.

7.2.2 Control of Internal Processing

Mitigation of internal processing risks will be accomplished by incorporating validation checks into systems that will detect corruptions from processing errors or vandalism. These controls will protect the integrity of the organization's information systems by building security into the organization's application systems and by ensuring the data run through the systems is complete, correct and appropriate.

Prior to implementation, system owners should ensure that applications are designed and implemented with restrictions that minimize the risk of processing failures that would undermine the integrity of the organization's information.

Controls will be in place to:

- Manage the location and use of add and delete functions to change data
- Prevent programs from running in the wrong order
- Prevent programs from running after a prior processing failure (see 5.1.1)
- Ensure the use of correct programs to recover from failures and ensure the correct processing of data
- Other actions to protect the integrity of application systems may include:
- Performing system or batch controls to reconcile data file balances after transaction updates
- Instituting balancing controls to check opening balances against previous closing balances
- Validating system-generated data (see 7.2.1)
- Performing checks on the integrity of data or software that is uploaded or downloaded, as applicable. Hash totals of records and files may be maintained.
- Performing checks to ensure that applications are run at the correct time order and terminate in case of failure.

7.2.3 Output Data Validation

All output of data from application systems will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Output data shall be checked for plausibility and reasonableness.

Output data counts shall be reconciled to ensure all data was processed.

Output data shall provide the reader with enough information that they can determine accuracy, completeness, precision and data classification (see **Error! Reference source not found.**).

Application owners will document procedures for responding to output validation tests and user responsibilities and will ensure that all users are trained on output validation policies and procedures.

7.3 Cryptographic Controls

7.3.1 Policy on the Use of Cryptographic Controls

The purpose of this policy is for ZESTIOT to assess the appropriateness of cryptography in the organization and if deemed appropriate implement policies standards and controls for its use. In addition, encryption is subject to certain export-control laws when used outside the United States (see 8.1)

Only ZESTIOT-approved uses of cryptography (encryption of any form) are allowed. This includes the methods of use (disk encryption, digital signatures, etc.) as well as algorithms or key strengths to be used. The IT Head, in conjunction with the Legal Officer, must authorize encryption products before being used.

Information to consider in the use of any encryption product includes:

- General principles under which business information should be protected
- The determination of the appropriate levels of cryptographic controls to be used
- Selection of appropriate methodology (private keys or public keys)
- Key management
- Recovery of information when keys are lost, compromised or damaged
- Roles and responsibilities for implementation
- Roles and responsibilities for key management
- Specific policies for use
- Implementation of policies for use

The Director – Digital Solutions will publish a list of approved encryption products, their approved uses, and standards for their configuration and use. These standards will consider the considerations listed above.

7.3.2 Encryption

ZESTIOT considers the use of encryption appropriate for protecting the information resources of the company in approved circumstances. The purpose of this policy is to regulate the use of encryption for the protection of sensitive or confidential data resources while ensuring that its use is proper and effective.

A risk assessment will be done for any highly sensitive information, and will include:

- The need for encryption.
- The implementation of encryption.
- Policies for encryption.
- The appropriate level of sophistication of the encryption algorithms chosen.
- The appropriate lengths of keys to be used.

The Head – Technology shall seek legal advice for issues that relate to the proper and legal use of encryption. The Legal Officer will consider national regulations concerning the trans-border flow of encrypted information, and export and import of encryption technology.

The organization shall seek the advice of specialists to select the correct products, design and implement the correct algorithms and key management programs, as appropriate.

7.3.3 Digital Signatures

ZESTIOT will consider the appropriateness of the use of digital signatures to protect and authenticate the integrity electronic documents. The Director – Digital Solutions shall assess the need for various cryptographic tools related to digital signatures.

The Director – Digital Solutions and those managers that are involved with electronic commerce will accomplish a risk assessment to assess the need for guaranteed message authentication and integrity. The risk assessment will cover:

- The use and cooperation of use among the organization's trading partners
- Necessary contracts and agreements between trading partners
- Documents appropriate for digital signature cryptography
- Key security (see 7.3.5)
- Key Management (see 7.3.5)
- Use of different keys than those that are used with encryption (see 7.3.2)
- Relevant legislation on the use of and legal standing of digital signatures

The Director – Digital Solutions will publish standards and guidelines concerning the use of digital signatures where they are deemed necessary or desired.

7.3.4 Non-repudiation Services

In support of digital signatures, ZESTIOT will consider non-repudiation services where necessary. The purpose of this policy is to anticipate and have a mechanism in place for the resolution of disputes regarding the substantiation of a receipt of a digitally signed document, prior to the dispute.

If necessary, the Director – Digital Solutions will publish standards and guidelines concerning support services for non-repudiation of digital signatures. These standards and guidelines should include:

- Establishing identification and ownership of digital certificates and private keys
- Generation of truly private keys (i.e., only the owner has ever had access to the private key)
- Safeguarding private keys (i.e., tamper-proof storage, physical security, etc.)

7.3.5 Key Management

The weakest component of any cryptographic solution is the protection of the encryption keys. To ensure the protection of cryptographic keys, both public and private keys, ZESTIOT will enact policies and procedures concerning key management. Key management policies and procedures will protect all keys from modification, destruction and unauthorized disclosure that could lead to a compromise in the authenticity, integrity and confidentiality of information.

7.3.5.1 Protecting Encryption Keys and Systems

A management plan and system shall be in place for the use of public and private keys that ensures the confidentiality and integrity of the private keys.

Keys shall be changed immediately if it is suspected that the keys were compromised. This may entail re-encrypting stored data with new secret or public keys.

All application systems that are using cryptography shall have different keys, and the application owner shall be responsible for generating and managing the keys in accordance with this policy and any applicable standards and guidelines published by the Information Security Office.

A list of systems that require keys shall be kept and evaluated periodically to ensure the accuracy and relevancy of the list.

Keys will be distributed and stored in a secure manner. Old versions of keys (i.e., keys that have been revoked) will be maintained in a secure manner to cover eventualities where data may have been encrypted with these keys before their revocation and have not been switched to new keys.

7.3.5.2 Key Management Standards

The Director – Digital Solutions shall establish standards, procedures and methods for key management. These standards will include the following:

- Secure procedures for key obtaining and storing keys
- Establishing and documenting the rules for changing and updating keys.
- Procedures for dealing with compromised keys or keys that have been revoked or deactivated.
- Secure procedures for destroying keys, including how and by what method.
- Secure procedures for key management business continuity including:
  - Recovering lost or corrupted keys
  - Supplier provisions for system loss
  - Archiving keys for achieved or backed-up information after keys have been changed
- Secure procedures for legal issues including:
  - Requests for access to cryptographic keys (in the case of unencrypted information requirements in court proceedings)
  - Legal agreements with suppliers of cryptographic services (including liability, reliability and response times)
  - Legal agreements with trading partners
- Secure procedures for establishing and defining the relationship between ZESTIOT and a trusted third-party certification authority for the protection of public keys, if used.

7.4 Security in Development and Support Processes

7.4.1 Software Change Control Procedures

Software development at ZESTIOT will utilize formal change control procedures for any changes to software. This process shall be integrated with the operational change control procedures (see 5.1.2). The purpose of this policy is to ensure that the security, availability and integrity of system software, systems and information are not compromised when there are changes to software.

The application owners shall be responsible for overseeing the security and control procedures of all changes to their applications. All software changes require formal approval by the application owner. All changes to software will be documented.

Application owners and the Director – Digital Solutions shall be responsible for insuring that programmers are only given access to areas of the application that are necessary for the approved work.

Application owners shall oversee the entire application change process prior to change including:

- Maintaining a record of agreed upon authorization levels
- Ensuring changes are submitted by authorized users
- Performing risk assessment to assure that controls and integrity procedures will not be compromised by changes, that business interruption is kept to an acceptable minimum and that the timing is appropriate for the change
- Identifying all software, information, databases and hardware that require change
- Obtaining formal and detailed proposals and specifications before work commences
- Obtaining formal approval prior to work commencing

Application owners shall oversee the entire application change process during the change including:

- Ensuring change minimized business interruption
- Documentation is updated and old documentation is archived
- Version control is maintained
- Maintaining an audit log of all change requests
- Updating all user procedures
- Ensuring that users accept all changes prior to implementation

Application owners shall oversee the entire application change process after the change including:

- Ensuring that testing is done securely (in a test environment that is segregated from development and operational systems)
- Ensuring that implementation does not disrupt business processes

7.4.1.1 Patch Management Process

ZESTIOT IT will institute a Patch Management process for operating systems and commercial software that will include the following elements:

- Identification of new patch availability
- Assessment of applicability and criticality of patches
- Patching effort timing and methods

- Effects of patches on existing applications
- Testing of patches before deployment
- Documentation of patch levels for various systems and applications

7.4.2 Technical Review of Operating System Changes

ZESTIOT IT shall review and test all new operating system changes or updates prior to installing them in an operation environment. This will ensure that operational integrity is maintained and that the organization's security requirements are met by any new operating system release.

A risk assessment shall be performed prior to the change of any of the organization's operating systems that shall include:

- Application control and integrity procedures – will they be compromised by operating system changes?
- Annual support plan and budget – will this cover testing of the new operating system?
- Timing of change – is there enough time to thoroughly test and review new operating system changes?
- Business continuity plans – have they been modified to accommodate changes.

Whenever possible, operating systems shall be maintained at a level supported by the vendor.

7.4.3 Restrictions on Changes to Software Packages

To ensure integrity and security of vendor supplied software packages, as well as to minimize the expense and support issues associated with modified products, ZESTIOT will use standard, unmodified vendor supplied software programs whenever possible.

If modifications must be made, the organization shall do a risk assessment to clarify and control the following issues:

- Compromise of built in controls and integrity processes
- Vendor requirements for consent
- Impact of future maintenance (Is vendor support still available or will the organization be responsible?)

Whenever possible the organization shall request that the vendor makes changes part of a future standard release.

If changes must be made, an original copy of standard software shall be retained, and the changes clearly documented in the operational copy.

All changes shall be thoroughly tested prior to use.

All changes shall be clearly documented in case there is a need to reapply the changes.

7.4.4 Covert Channels and Trojan Code

To prevent damage to ZESTIOT systems and applications, ZESTIOT will actively protect its information assets from covert channels and Trojan code.

The organization will follow the following procedures when acquiring software:

- All programs will be a acquired from reputable sources
- All programs will be acquired in source code (if available)
- All programs that are acquired will have source code verified
- All products shall have source code inspected prior to operational use
- All programs that are acquired shall be evaluated products

Access shall be that which is allowed in ZESTIOT.'s access control policy (see 6.1).

Modification to code, if necessary, shall be controlled, monitored, inspected, and only done by those staff members that have proven their trustworthiness to work on key systems.

8.0 COMPLIANCE

8.1 Compliance with Legal Requirements

8.1.1 Identification of Applicable Legislation

To avoid any legal or security breaches, ZESTIOT will define, document, and comply with all relevant statutory, regulatory, and contractual requirements for each information system.

Each system owner shall implement controls to comply with all relevant statutory, regulatory and contractual requirements for their information system.

System owners shall seek the advice of the Legal or Director – Digital Solutions for all relevant legal and security information.

Care shall be taken to account for different requirements in different locations (i.e. issues associated with encryption, see 7.3). ZESTIOT.'s Legal Officer will determine differences from standing policy for those locations that have differing legal requirements and will work with the Director – Digital Solutions to create exceptions to general policy and specific policies for those jurisdictions.

8.1.2 Intellectual Property Rights

All users at ZESTIOT will comply with the legal aspects of intellectual property protection and the rights and limitations of license agreements associated with proprietary software products.

The purpose of the policy is to ensure that users are aware of and comply with such restrictions as copyrights, trademarks, and design rights. Users are responsible for not violating applicable copyright, intellectual property, or other licensing rights of electronic media or software that is not the property of ZESTIOT. Furthermore, users are responsible for not using ZESTIOT intellectual property outside the limits of ZESTIOT policy or licensing.

Failure to abide by these policies will subject the user to disciplinary actions up to and including termination or criminal/civil charges.

8.1.2.1 Intellectual Property Standards and Training

IT will publish the organization's standards for software acquisition (see 7.4).

Intellectual Property Rights Protection policies shall be included in all security awareness training (see 3.2).

The Director – Digital Solutions, along with each system owner, shall establish, document and educate applicable users on:

- Maintaining appropriate asset registries

- Maintaining proof of ownership or licenses
- Implementing controls to restrict the number of users to the appropriate licensed amount
- Implementing controls and checks to ensure that only licensed software is installed
- Policies and controls to assure that license conditions are met
- Policies and controls for disposing of or transferring software to others
- Use of appropriate audit tools

8.1.2.2 Using Software from Outside Sources

IT will publish the organization's policies and procedures for obtaining software from public networks (see 8.7.6).

Users will not download or install any third-party pirated software on ZESTIOT systems.

Users will not download or install any non-approved software from the Internet. The Director – Digital Solutions will approve specific software for use from the Internet if there is a business need.

8.1.2.3 Copyrighted Material and Peer-To-Peer File Sharing at ZESTIOT

ZESTIOT respects the copyrights of those involved in creating and distributing copyrighted material, including music, movies, software, and other literary and artistic works. It is the policy of ZESTIOT to fully comply with all copyright laws.

ZESTIOT provides its employees access to computer systems and the Internet to allow them to do their jobs on behalf of ZESTIOT. Employees may make occasional use of the Company's computer systems and network for personal use

When ZESTIOT employees need to use copyrighted materials to do their jobs, ZESTIOT acquires appropriate licenses.

ZESTIOT employees may not:

- store or otherwise make unauthorized copies of copyrighted material on or using ZESTIOT computer systems, networks, or storage media.
- download, upload, transmit, make available or otherwise distribute copyrighted material using ZESTIOT.'s computer systems, networks or storage media without authorization; or
- use or operate any unlicensed peer-to-peer file transfer service using ZESTIOT.'s computer systems or networks or take other actions likely to promote or lead to copyright infringement.

Please note – this is not a policy against MP3 files, or electronic music and video files as such. Rather, the policy is targeted at unauthorized – that is, unlicensed – electronic music and video files. If you

downloaded the files from an unlicensed peer-to-peer site or other source, then those files are almost certainly not authorized and most likely violate the copyright laws.

ZESTIOT reserves the right to:

- Monitor its computer systems, networks, and storage media for compliance with this and other Company policies at any time, without notice and with or without cause; and
- Delete from its computer systems and storage media, or restrict access to, any unauthorized copies of copyrighted materials it may find, at any time and with or without notice.

8.1.3 Data Protection and Privacy of Personal Information

ZESTIOT will comply with all applicable laws and regulations regarding the protection of personal data. This will ensure that ZESTIOT is collecting personal information (that information that can be used to identify living individuals) in a manner that complies with laws as well as processing and disseminating that data in a lawful manner.

The Director – Digital Solutions or a nominated information protection officer shall document policies and procedures that comply with applicable laws and regulations for the handling of personal information for each such instance.

The Director – Digital Solutions shall distribute policies and educate users, managers and service providers on their responsibilities for compliance.

Information owners shall inform the appropriate information protection officer about proposals to keep information in a structured file. The information protection officer shall advise information owners on policies and procedures concerning their protection and storage of such data.

Confidential information entrusted to ZESTIOT by members, business partners, suppliers, and other third parties shall be protected in accordance with ZESTIOT.'s Security Policies and shall be protected with at least the same care as ZESTIOT.'s confidential information.

8.1.4 Prevention of Misuse of Information Processing Facilities

Users of ZESTIOT information processing facilities will utilize these facilities for only management-authorized business purposes. ZESTIOT reserves the right to legally monitor facilities for compliance. The purpose of this policy is to protect the availability and integrity of the organization's information processing facilities as well as protect the organization against legal sanction against the misuse of computers.

The Director – Digital Solutions shall provide managers with guidelines for the legal monitoring of computer facilities.

Managers of information processing facilities shall monitor the use of such facilities.

If misuse is detected, it shall be brought to the attention of the person's manager for disciplinary action.

An acceptable use policy will be communicated to users. This policy will be included in the acceptance of policy letter that employees will sign during orientation. The acceptable use policy will govern permitted and forbidden activities for their location. In all cases, any activity not expressly permitted is forbidden.

At logon, a message shall appear to warn users that they are entering a private system and that unauthorized access is not permitted.

8.1.5 Regulation of Cryptographic Controls

Cryptographic solutions are governed by various export control and use laws and regulations, which vary from country to country. ZESTIOT will comply with all applicable agreements, laws, regulations or other instruments that control the use or access of cryptographic controls.

The Legal Officer shall document the restrictions on the use of cryptographic controls including:

- Import and export restrictions on cryptographic software or hardware.
- Import and export restrictions on software or hardware that can have cryptographic functions added to it.
- Mandatory of discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content; and
- National laws.

The Director – Digital Solutions shall publish, distribute, and educate users on applicable restrictions.

Before any encrypted information or cryptographic controls are sent to another country the Legal Officer shall be consulted.

8.2 Reviews of Security Policy and Technical Compliance

8.2.1 Compliance with Security Policy

To maintain the security, integrity and availability of the organization's information processing assets, ZESTIOT will continually monitor the organization's compliance with its security policies.

The Director – Digital Solutions shall ensure that an annual internal audit takes place. The scope of this audit is a Security Posture assessment for all external/internal routers, firewalls, access points, hosts and offsite facilities for Disaster Recovery and media storage.

Managers shall continually monitor their user's compliance with the organization's security policies, procedures, standards and requirements (for information on monitoring see 6.7).

8.2.2 Technical Compliance Checking

The Director – Digital Solutions will monitor the organization's technical compliance with its security implementation standards.

A specialist shall be used for technical compliance checking to ensure that hardware and software security controls have successfully been implemented in operational systems.

The technical compliance checking will be done manually (by a qualified system engineer), with automated software tools or in combination.

A qualified technical specialist shall interpret results of subsequent technical reports.

Penetration testing shall be done by third party experts as necessary (care shall be take that a successful penetration test does not compromise they system or exploit other vulnerabilities).

The Director – Digital Solutions shall oversee all technical compliance testing.

8.3 System Audit Considerations

8.3.1 System Audit Controls

Any agency conducting system audits will carefully plan, agree upon, and expedite system audits to minimize the risk of disruptions to operational business processes. This will ensure the organizations security requirement compliance while maximizing the availability, integrity and security of the organization's information resources.

The scope and requirements of all audits shall be controlled and agreed to by management.

Access to any files beyond read only shall be approved by Technology Head. This includes isolated copies of system files. If isolated copies of system files are used, the files shall be destroyed as soon as the audit is completed.

Requirements for additional testing shall be identified and agreed upon by appropriate management.

IT resources shall be identified and made explicitly available for audit assistance.

All access to system shall be logged to produce a reference trail.

All procedures, responsibilities, requirements and scope shall be documented.

8.3.2 Protection of System Audit Tools

Any agency conducting system audits will protect access to system audit tools (i.e. software or data files). This will protect the security, availability and integrity of the organization's information resources by ensuring that the organization's system audit tools are protected from misuse or compromise.

System audit tools shall be separated from operational and development systems unless they are given the added appropriate protection and are authorized by the Director – Digital Solutions.

Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance by the Director of Information Security (see 3.3.2).

9.0 CLOUD SECURITY

9.1.0 Essential Points

Network segmentation:

in multitenant environments, assess what segmentation is in place between ZESTIOT resources and those of other customers, as well as between ZESTIOT own instances. Leverage a zone approach to isolate instances, containers, applications, and full systems from each other when possible.

Identity and privileged access management:

Enforce least privilege to restrict access and to harden cloud resources (for instance, only expose resources to the Internet as is necessary, and de-activate unneeded capabilities/features) All facets of computing in the cloud should use access control lists (ACL). Ensure privileges are role-based, and that privileged access is audited.

Discover and onboard cloud instances and assets:

Once cloud instances and services are discovered and grouped, bring them under management (i.e. managing and cycling passwords, etc.). Discovery and onboarding should be automated as much as possible so that shadow IT cloud resources and accounts aren't able to arise and proliferate.

User activity monitoring:

Track how your users are using your cloud environment.

Password control (privileged and non-privileged passwords):

Never allow the use of shared passwords. Ensure password management best practices (refer password Policy)

Vulnerability management:

Regularly scan for vulnerability and privilege-related risks. Perform penetration testing to determine real-world security resilience. And, carry out security audits and testing to identify vulnerabilities.

Patching and maintenance:

Ensure your cloud vendor has a reliable approach to patch known vulnerabilities. Also, be proactive in scanning for and patching known vulnerabilities across your own infrastructure.

Encryption:

Ensure your cloud data is encrypted, at rest, and in transit.

Alerts and reporting:

See what reporting is available through your cloud vendor(s) and use a SIEM or similar tool to integrate and centralize it with data from in-house and other vendor solutions as much as possible. A holistic approach to identify what is happening in ZESTIOT environment.

Disaster recovery:

Depends on business requirement and application criticality, disaster management service will be subscribed.

Monitoring:

A continual security monitoring approach should be in place across all environments and instances.

Technical Controls:

ZESTIOT must implement firewalls, intrusion prevention, application layer firewalls and encryption

ZESTIOT should implement controls to prevent and not limited to distributed denial of service attack protection, password attacks and data protection.

Breach Notification:

Cloud service provider or application support team (SAAS) must notify ZESTIOT within 24 hours of a potential or actual breach or incident that may affect ZESTIOT environment.

Cloud service provider or application support team (SAAS) notify the province of any changes to security policies, procedures, or agreements.

9.1.1 Cloud Security

Security and Audit Solution:

Cloud Security Center is a unified infrastructure security management system that strengthens the security posture of data centers, and provides advanced threat protection across ZESTIOT hybrid workloads in the cloud

Cloud Security Center enables to strengthen ZESTIOT security posture. This means it helps to identify and perform the hardening tasks recommended as security best practices and implement them across ZESTIOT machines, data services, and apps. ZESTIOT will be maintaining more than 0% secure score. Anything less than 60% will be treated as risk and risk mitigation will be applied immediately.

Network map

Network map service will provide the security status of ZESTIOT's network. The map enables ZESTIOT to see the topology of workloads and it provide each node configuration status. We can see how ZESTIOT nodes are connected, which helps to block unwanted connections that could potentially make it easier for an attacker to creep along your network

Protect against threats:

Security Center's threat protection includes fusion kill-chain analysis, which automatically correlates alerts in your environment based on cyber kill-chain analysis, to help you better understand the full story of an attack campaign, where it started and what kind of impact it had on your resources.

Block brute force attacks:

Security Center helps to limit exposure to brute force attacks. By reducing access to virtual machine ports, using the just-in-time VM access, ZESTIOT harden the network by preventing unnecessary access. ZESTIOT has set secure access policies on selected ports, for only authorized users, allowed source IP address ranges or IP addresses, and for a limited amount of time.

Protect IoT:

Cloud Defender for IoT provides threat prevention and analysis for every device, IoT Edge and IoT Hub, across to IoT assets. Defender for IoT simplifies hybrid workload protection by delivering unified visibility and control, adaptive threat prevention, and intelligent threat detection and response across workloads running on edge, on-premises, in Cloud, and in other clouds.

Resource Manager:

It will help to deploy, manage, and monitor all the services for solution as a group, rather than handling these services individually. Access control to all resources in ZESTIOT resource group, and those policies are automatically applied when new resources are added to the resource group. define the dependencies between resources so they're deployed in the correct order.

Cloud Monitor:

Cloud Monitor offers visualization, query, routing, alerting, auto scale, and automation on data both from the infrastructure (Activity Log) and each individual resource (Diagnostic Logs). Monitor is used to alert security-related events that are generated in logs.

Monitor logs:

Monitor logs is useful tool in forensic and other security analysis, as the tool enables to quickly search through large amounts of security-related entries with a flexible query approach.

Web Application firewall:

The web application firewall (WAF) in Cloud Application Gateway helps protect web applications from common web-based attacks like SQL injection, cross-site scripting attacks, and session hijacking. It comes preconfigured with protection from threats identified by the Open Web Application Security Project (OWASP).

Role-Based Access Control (RBAC):

Restricting access based on the need to know and least privilege security principles is imperative for to enforce Security policies for data access. These access rights are granted by assigning the appropriate Cloud role to groups and applications at a certain scope. Cloud built-in roles, such as Storage Account Contributor, to assign privileges to users. Access to the storage keys for a storage account using the Cloud Resource Manager model can be controlled through Role-Based Access Control (RBAC).

Shared Access Signature:

A shared access signature (SAS) provides delegated access to resources in storage account. The SAS means that grant a client limited permission to objects in ZESTIOT storage account for a specified period and with a specified set of permissions. Limited period access to outsiders will be provided with appropriate approval from Director – Digital Solutions and for only limited period.

Encryption in Transit:

Encryption in transit is a mechanism of protecting data when it is transmitted across networks. With Cloud Storage, secure data can be achieved by using:

- Transport-level encryption, such as HTTPS when you transfer data into or out of Cloud Storage.
- Wire encryption, such as SMB 3.0 encryption for Cloud File shares.
- Client-side encryption, to encrypt the data before it is transferred into storage and to decrypt the data after it is transferred out of storage.

Encryption at rest:

Data encryption at rest is a mandatory step towards data privacy, compliance, and data sovereignty. Cloud storage security features that provide encryption of data that is “at rest”:

- Storage Service Encryption allows to request that the storage service automatically encrypt data when writing it to Cloud Storage.
- Client-side Encryption also provides the feature of encryption at rest.
- Cloud Disk Encryption allows to encrypt the OS disks and data disks used by an IaaS virtual machine.

Network Layer Controls:

Network access control is the act of limiting connectivity to and from specific devices or subnets and represents the core of network security. The goal of network access control is to make sure that ZESTIOT virtual machines and services are accessible to only users and devices to which you want them accessible.

Network Security Groups:

A Network Security Group (NSG) is a basic stateful packet filtering firewall and it enables to control access based on a 5-tuple.They can be used to control traffic moving between subnets within an Cloud Virtual Network and traffic between an Cloud Virtual Network and the Internet.

Cloud Virtual Network:

An Cloud virtual network is a logical isolation of the Cloud network fabric dedicated to subscription. It controls the IP address blocks, DNS settings, security policies, and route tables within the network. it segments VNet into subnets and place Cloud IaaS virtual machines (VMs) and/or Cloud services (PaaS role instances) on Cloud Virtual Networks.

VPN Gateway:

To send network traffic between your Cloud Virtual Network and on-premises / outside site, create a VPN gateway for Cloud Virtual Network. A VPN gateway is a type of virtual network gateway that sends encrypted traffic across a public connection.

Traffic Manager:

Traffic Manager provides a range of traffic-routing methods to suit different application needs, endpoint health monitoring, and automatic failover. Traffic Manager is resilient to failure, including the failure of an entire Cloud region.

Cloud Load Balancer:

Cloud Load Balancer delivers high availability and network performance to applications. It is a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy instances of services defined in a load-balanced set. Cloud Load Balancer can be configured to:

- Load balance incoming Internet traffic to virtual machines. This configuration is known as public load balancing.
- Load balance traffic between virtual machines in a virtual network, between virtual machines in cloud services.

Virtual machine backup:

Application errors can corrupt your data, and human errors can introduce bugs into applications that can lead to security issues. With Cloud Backup, your virtual machines running Windows and Linux are protected.

Cloud Site Recovery:

Cloud Site Recovery helps orchestrate replication, failover, and recovery of workloads and apps so that they are available from a secondary location if primary location goes down.

Secure Identity:

Cloud uses multiple security practices and technologies across its products and services to manage identity and access.

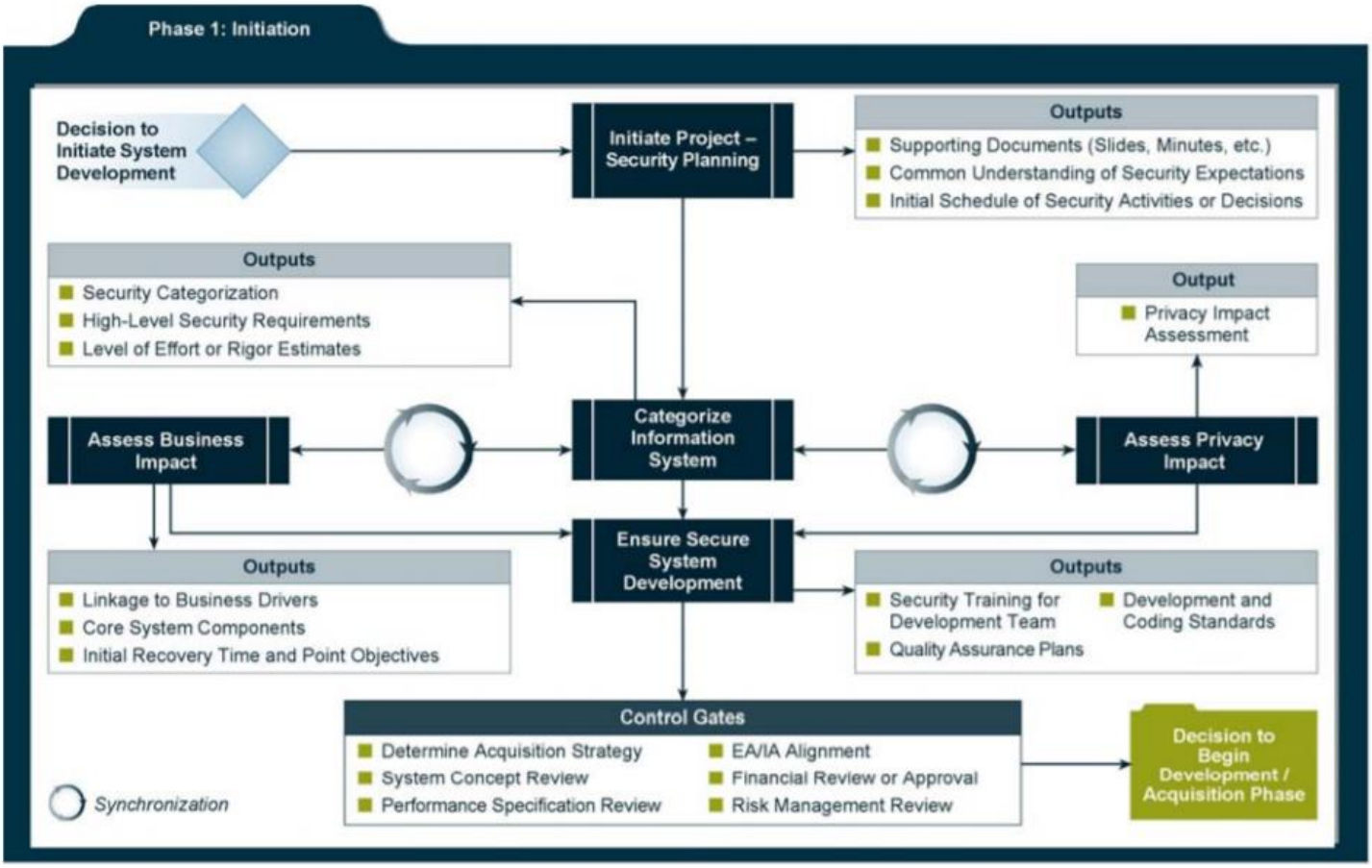
- Multi-Factor Authentication provides strong authentication with a range of easy verification options, while accommodating users with a simple sign-in process.
- Cloud Authenticator provides a user-friendly Multi-Factor Authentication experience that works with both Cloud Active Directory and Cloud accounts.
- Password policy enforcement increases the security of traditional passwords by imposing length and complexity requirements, forced periodic rotation, and account lockout after failed authentication attempts.
- Token-based authentication enables authentication via Cloud Active Directory.
- Cloud role-based access control (Cloud RBAC) enables you to grant access based on the user's assigned role.

10.0 SDLC (SOFTWARE DEVELOPMENT LIFE CYCLE)

Introduction:

This section describes several security considerations that will help integrate information security into the SDLC. Security considerations are identified in each SDLC phase, thus advancing the business application and security requirements together to ensure a balanced approach during development.

10.1.1 SDLC Phase: Initiation



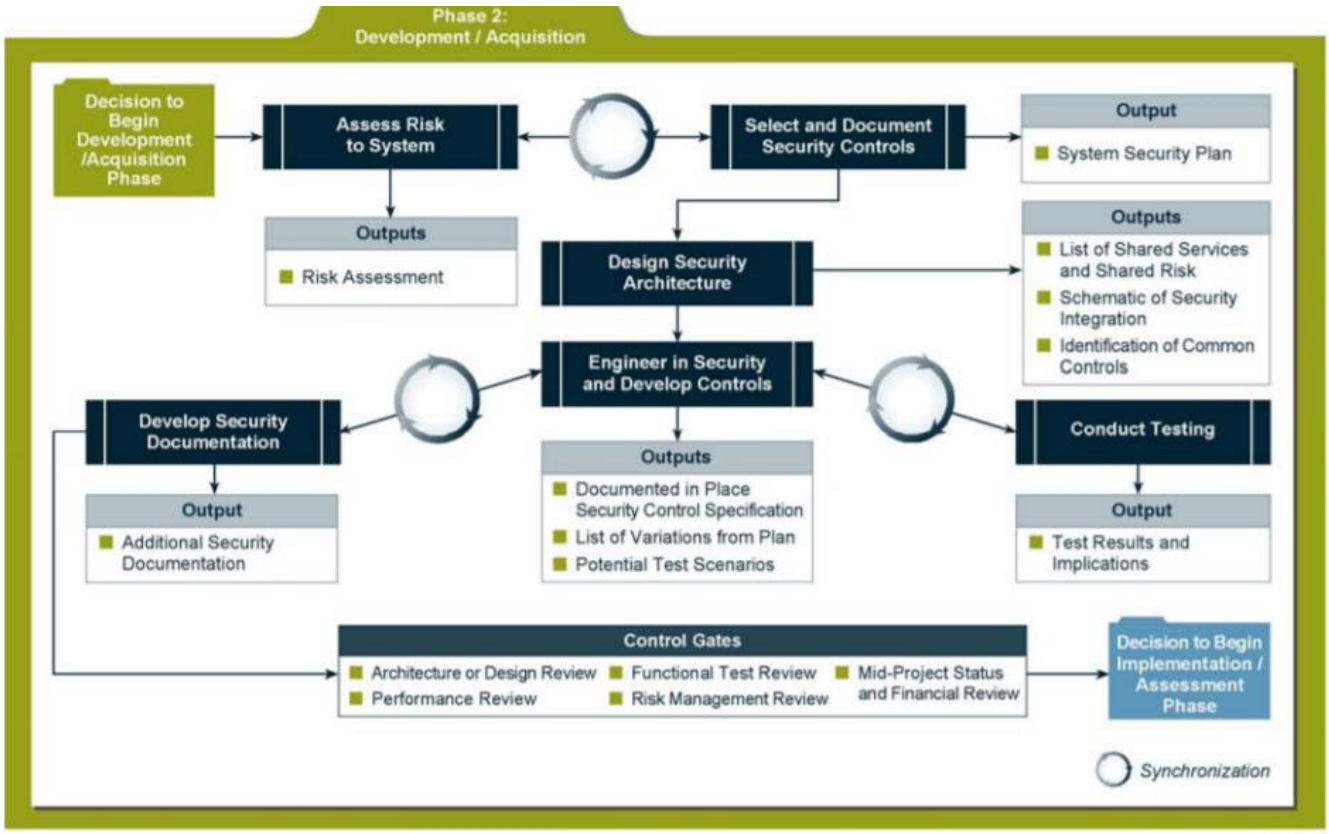
During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. At this point, security is looked at more in terms of business risks with input

from the information security office. Initial delineation of business requirements in terms of confidentiality, integrity, and availability.

10.1.2 Controls

- A determination of the acquisition strategy to be used throughout the remainder of the development process.
- A system concept review that verifies that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints.
- A performance specification review that ensures that the initial system design has addressed all currently identified specified security requirements.
- An enterprise architecture (EA) alignment that harmonizes IT vision, standards, and business requirements, as well as security alignment with current and imminent security services.
- A financial review that verifies that the system will be aligned with ZESTIOT standard and guidance while balancing the cost implications associated with risk management; and
- A risk management review that conforms to the recommended risk management framework guidelines to reduce ambiguity in managing system risk.

10.1.3 SDLC Phase: Development/Acquisition



This section addresses security considerations unique to the second SDLC phase.

Key security activities for this phase include.

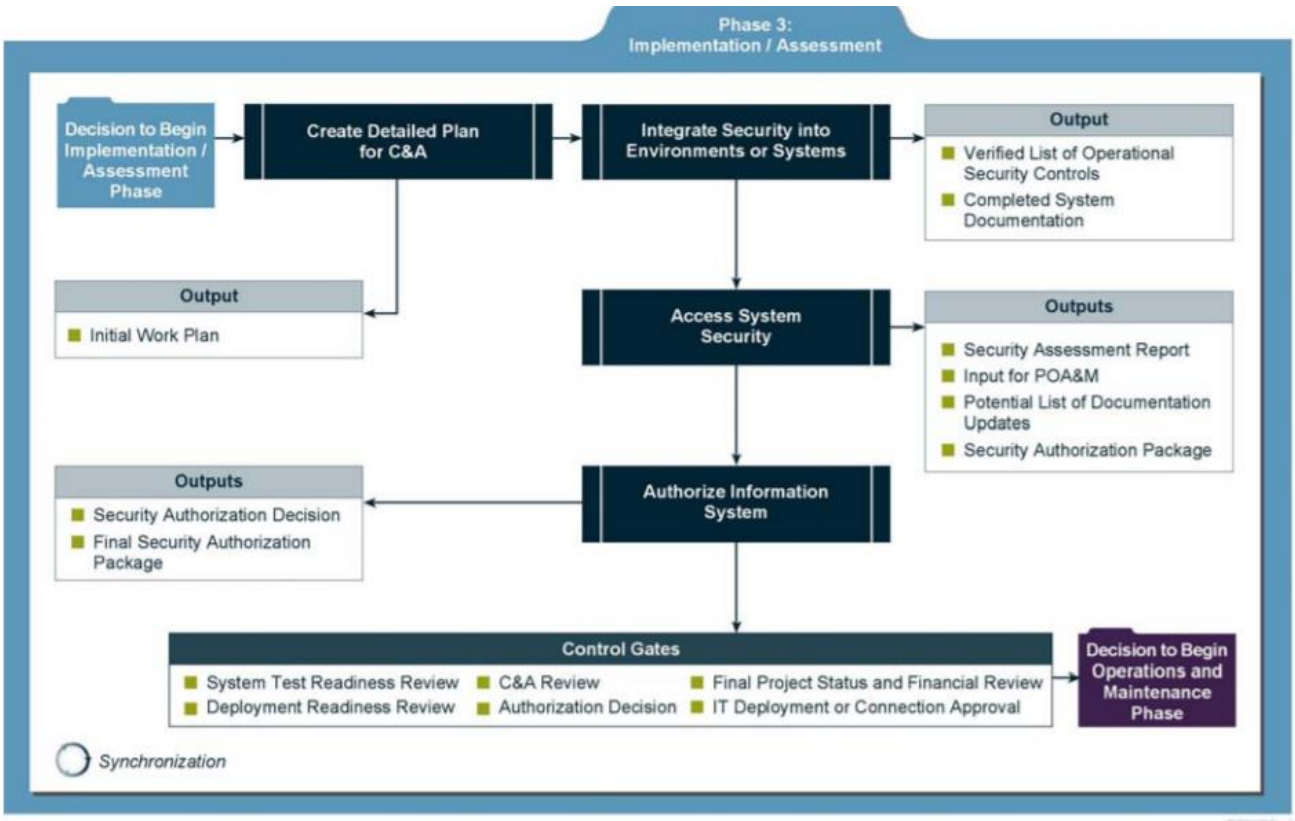
- Conduct the risk assessment and use the results to supplement the baseline security controls.
- Analyze security requirements.
- Perform functional and security testing.
- Prepare initial documents for system certification and accreditation.
- Design security architecture.

10.1.4 Controls

- An Architecture/Design Review that evaluates the planned system design and potential integration with other systems as well as incorporation of shared services and common security controls, such as authentication, disaster recovery, intrusion detection, or incident reporting.

- A system Performance Review that evaluates whether the system is delivering, or capable of delivering, to the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use.
- A system Functional Review that ensures functional requirements identified are sufficiently detailed and are testable.
- Mid-Project Status & Financial Review is important to detect major shifts in planned level of effort to ensure cost-benefit ratios are monitored and effective decisions are continued.
- A follow-on review of risk management decisions may be needed if, due to the aforementioned reviews, the system and/or its security controls and/or its requirements change.

10.1.5 SDLC Phase: Implementation / Assessment



Implementation/Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization's operational environment.

Key security activities for this phase include:

- Integrate the information system into its environment.
- Plan and conduct system certification activities in synchronization with testing of security controls.
- Complete system accreditation activities.

10.1.6 Controls

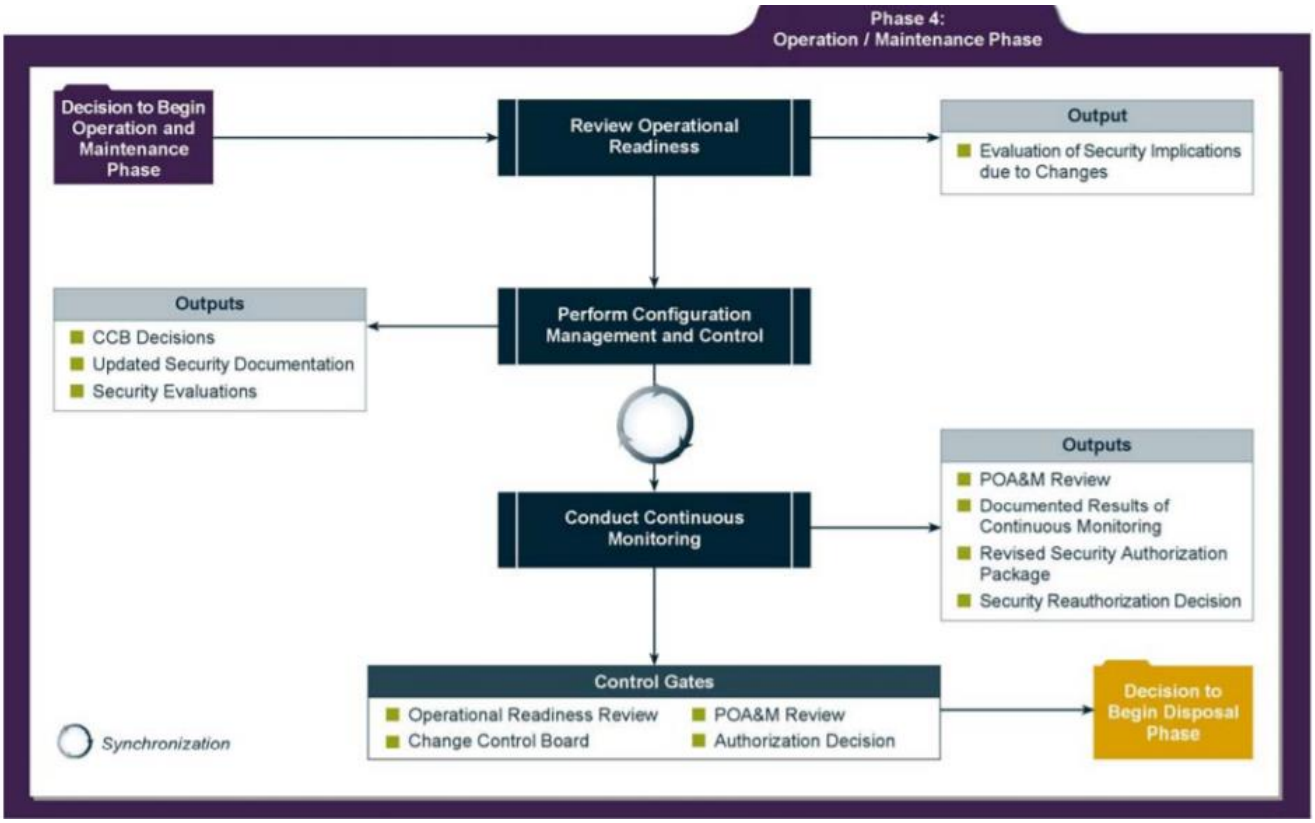
General types of control gates for this phase may include:

System Test Readiness Review

- C&A Review
- Final Project Status and Financial Review

- Deployment Readiness Review
- Authorizing Official (AO) Decision
- IT Deployment or Connection Approval.

10.1.7 SDLC Phase: Operations and Maintenance



Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced.

The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated.

The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient.

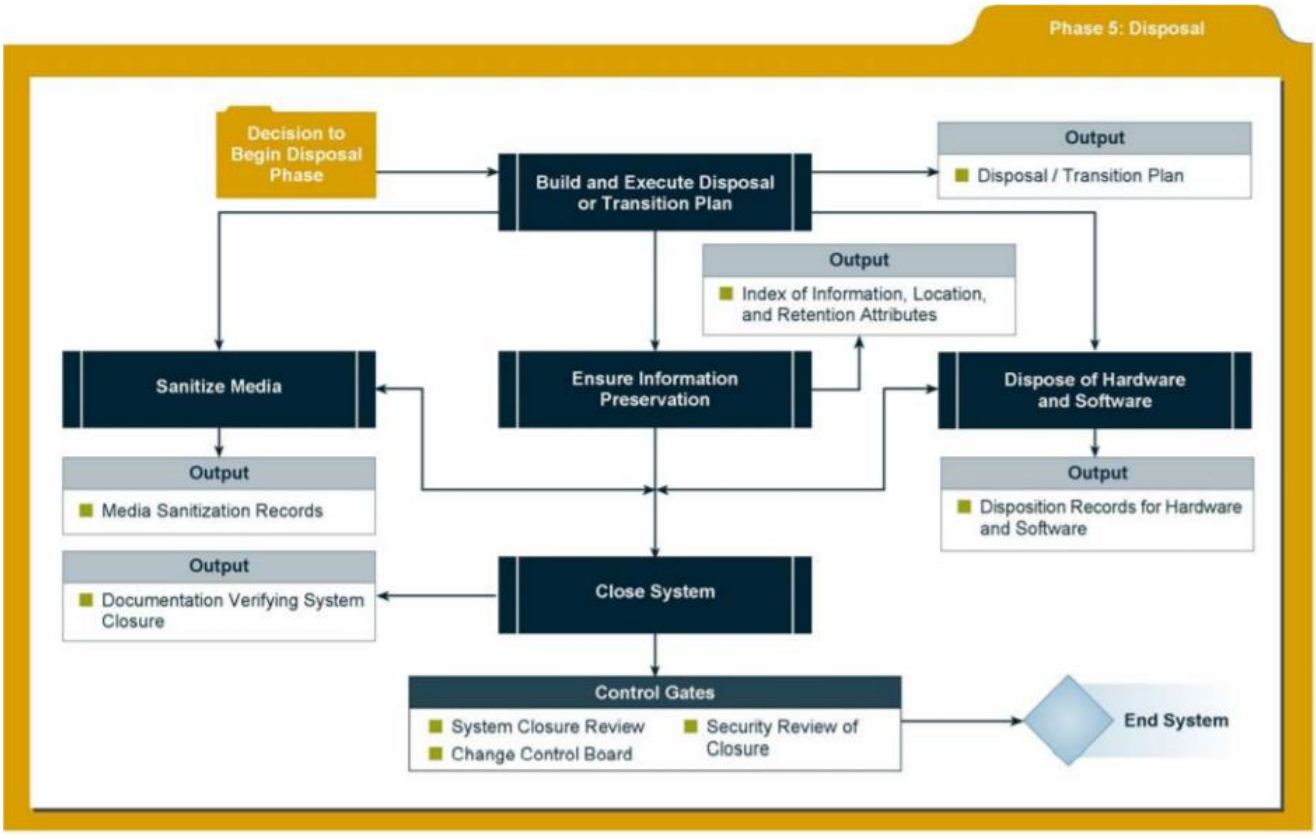
Operations continue if the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level.

10.1.8 Controls

General types of control gates for this phase may include:

- Operational Readiness Review
- Change Control Board Review of Proposed Changes
- Review
- Accreditation Decisions (Every three years or after a major system change)

10.1.9 SDLC Phase: Disposal



Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place.

Information security issues associated with information and system disposal should be addressed explicitly.

When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected

Key security activities for this phase include:

- Build and Execute a Disposal/Transition Plan.
- Archive of critical information.
- Sanitization of media.
- Disposal of hardware and software

10.1.10 Controls

General types of control gates for this phase may include:

- System Closure Review
- Change Control Board
- Security Review of Closure.