I. OVERVIEW

This policy and procedural manual (PPM) is intended to provide basic orientation information for the operational activities of the Village of Sea Ranch Lakes, Florida. It is not intended to be a detailed guide describing each aspect of the internal specific procedures. However, this manual is intended to provide sufficient procedural detail to enable the Village, other governmental entities, and the contractor/vendor community to:

a) be fully aware of, and comply with, Village Information Technology policies, and

b) effectively participate in the Village's Information Technology program.

This document applies to all Village of Sea Ranch Lakes users regardless of the user's location (e.g., in an office, at a customer site, on an airplane, at an information user's residence, at a shared location, etc.); this term includes all Village employees, and contractors/vendors that require access to Village information resources, authorized previously by the Village Clerk.

Continuous Improvement: The content of this document is subject to regular review based on input from Village of Sea Ranch Lakes staff.

II. DEFINITIONS

Information Resources: Electronic and non-electronic resources owned by the Village, including but not limited to: documentation (designs, research material, reports, specifications, contracts); electronic media (computer software, computer tapes, computer disks, computer printouts); business operations (inventions, methods, processes, work products, customer lists); business development (municipality information, operating plans, cost and financial data); and system resources (phone systems, organization- issued cellular phones, hardware, networking resources, operating systems).

Data: Information stored on hardware and accessed by using software.

Software: Programs and routines written in a symbolic language that control the functioning of the hardware.

Hardware: The physical, touchable, and material parts of a computer.

Third Parties: Vendors and business partners of the Village, bound by underpinning agreements or contracts with the Village.

Third Party Personnel: Representatives of vendors and business partners of the Village.

Remote Access: Any communication to the Village of Sea Ranch Lakes systems and applications from an external (remote) location or facility through a data link.

III. INFORMATION SECURITY POLICIES

A. PROHIBITED ACTIVITIES

Village of Sea Ranch Lakes information must be used only for the business purposes expressly authorized. The following list of activities are a minimum subset of prohibited activities.

Village of Sea Ranch Lakes expressly prohibits Village staff from:

a) Uploading, downloading, printing, transmitting, and viewing any information (image, sound, program, or document) that could be deemed offensive, derogatory, harassing, based on:

- Race,
- Gender,
- National Origin,
- Sexual Orientation,

- Religion,
- Political Belief,
- Disability,
- Age.

b) Uploading, downloading, printing, transmitting, and viewing any information (document, image, sound, or program) containing the following without Village and/or the author's authorization:

- Trade Secrets,
- Copyrighted Materials,
- Trademark Materials,
- Patented Materials,
- Other Confidential, Private or Proprietary Information or Materials, including all non-public Client material.

c) Using Village computers to:

- Forge (or attempt to forge) electronic mail messages,
- Obtain unauthorized access or conduct tampering of the electronic mail of others,
- Send harassing, obscene and/or other threatening e-mail to others,
- Send unsolicited junk mail, "for-profit" messages, or chain letter messages,
- Gain unauthorized access to any computer system, including remote computers or other systems in any way,
- Damage, alter, or disrupt any computer system, including remote computers or other systems in any way,
- Participate in illegal activities,
- Decrypt system or user passwords from any computer system, including remote computers or other systems in any way,
- Copy system files from any computer system, including remote computers or other systems in any way,
- Copy copyrighted materials, such as third-party software, without the expressed written permission of the owner or the proper license,
- Intentionally attempt to "crash" Network systems or programs,
- Attempt to secure a higher level of privilege on the Network,
- Willfully introduce computer programs into the organization Network or into external Networks,
- Willfully introduce computer viruses into the organization Network or into external Networks,
- Solicit business, sell products, or otherwise engage in commercial activities other than those required by their job responsibilities,
- Use anyone's code or password without authorization,
- Allow system access to non-Village personnel without supervisor's and Information Technology's permission,
- Jeopardize or breach the security of the Village computer systems in any way,
- Excessively use internet for non-Village related matters,
- Tamper with any of Village computer systems in any way.

IV. <u>INFORMATION SECURITY</u>

A. INFORMATION OWNERSHIP

All information, data and documentation gathered by, generated by, or provided by Village staff, in the course of their employment and/or utilizing organization owned assets for the Village's business purposes, are the property of the Village.

The Village of Sea Ranch Lakes has legal ownership of, or rights to, the contents of all files, information, and messages stored or transmitted on its computer and network systems, and reserves the right to examine all data stored in or transmitted by its computer and communications systems, without prior notice, whenever there is a business need which includes, but is not limited to, any investigation of unauthorized or inappropriate use of the systems or other investigation conducted with a business purpose. There should be no expectation of privacy associated with the information stored in or sent through Village systems.

The use of encryption, the labeling of an email or document as private, the deletion of an email or document, or any other such process or action, shall not diminish the organization's rights to examine and review such information in any manner, as stated above. Unauthorized use of passwords/encryption to prevent users from gaining access to a computer related resource is prohibited.

B. INFORMATION SECURITY INCIDENT REPORTING

Village staff must immediately report all suspected information security problems, vulnerabilities, unauthorized activity, and incidents to the Village Clerk. All suspected information security incidents must be reported as quickly as possible to the Village Clerk.

V. <u>ACCESS CONTROL AND AUTHENTICATION MECHANISMS</u>

A. ACCESS PHILOSOPHY

Access to Village information must be granted only when a legitimate business need has been demonstrated and access has been approved in advance by the Village staff's authorized supervisor. Network and/or system privileges of all users must be restricted based on the need for access.

B. DEFAULT FACILITIES

Village staff that require access to network services will be granted basic information systems services such as electronic mail and word processing facilities. All other system capabilities and access to specific applications must be specifically requested and approved by the Village Clerk. The existence of certain access privileges does not, in and of itself, mean that an individual is authorized to use these privileges. If Village staff have any questions about access control privileges, they must direct these questions to the Village Clerk.

C. DEPARTURES FROM THE VILLAGE OF SEA RANCH LAKES

Any change in the employment status of Village staff must be immediately reported to the Village Clerk. When a Village staff member leaves the organization, all system privileges and access to Village information must cease immediately. Departed Village staff must not be permitted to continue to maintain an electronic mail account with the Village, unless specifically authorized by the Village Clerk. All Village information disclosed to Village staff must be returned or destroyed. All work done by Village staff for the Village of Sea Ranch Lakes is Village property and will remain with the Village when Village staff depart.

D. UNIQUE USER IDs

Each Village staff will be assigned a unique user ID. All user IDs on Village networks/applications must be constructed according to the Village user ID construction standard and must clearly indicate the responsible individual's name. This user ID follows an individual as they move through the organization. It must be permanently decommissioned when a user leaves the Village. Re-use of user IDs is not permitted, with the exception of re-hiring.

Users are responsible for all activity that takes place with their user ID and password or other authentication mechanisms. User IDs are linked to specific people, and are not associated with computer terminals, departments, or job titles. With the exception of internet pages, intranet pages, and other places where anonymous interaction is both generally understood and expected, anonymous and guest user IDs are not permitted unless approved in advance by the Village Clerk.

The system privileges granted to every employee must be reevaluated every 12 months to determine whether currently enabled system privileges are needed to perform the user's current job duties.

The access for contractors and temporary workers will be set to expire after three months by default. The privileges of these Village staff must be immediately revoked by the Village Clerk when the project is complete, or when the contractor or temporary worker stops working with the Village. The Village Clerk must review the need for the continuing privileges of contractors and temporary workers every three months.

E. PASSWORD

a) Every workstation must have a password-protected screen saver.
b) Every user is held accountable of his/ her activity when using a Village workstation or when connected to the Village network.
c) Every user must keep his / her password confidential; it is forbidden to share user credentials to other users. All IT activity is traced by the Village Clerk.
d) If a user detects his/ her credentials have been compromised, the user must immediately change his/ her password, and proceed to notify the Village Clerk of this event.
e) User passwords must comply to the requirements below:

- Password minimum length: eight (8) characters.
- Password usage: must not be identical to the previous ten (10) passwords.
- Password validity: Ninety (90) days
- Password components restrictions: Password must contain at a minimum three of the following four items: alphanumeric characters (A-Z) upper case and/or lowercase, numeric characters (0-9), non-alphanumeric characters (symbols) ~!@#$%A&*() -+='O\{}I:;'"<,>.?/

VI. OPERATIONS

A. COMPUTER VIRUSES

All computers, servers, or network devices susceptible to computer virus infestation will be protected by corporate anti-virus programs. Virus screening software will be installed and enabled with real-time functionality on all Village local area network servers, and networked personal computers and will be configured to be automatically update virus definitions.

Any user who suspects infection by a virus must immediately shut-down the involved computer, disconnect from all networks, contact the Village Clerk, and make no attempt to eradicate the virus.

Users must not download software on any computer system property of the Village. Users must not install software on their workstation computers, network servers, or other machines without receiving advanced authorization to do so from the Village Clerk. Users will exercise extreme caution in downloading and executing any files attached to email.

B. CRITICAL DATA LOCATION

Village users must not store confidential or critical business information on workstation hard disk drives. This type of information must reside on security protected server shares.

C. SYSTEM LOGON BANNER

Logon screens for computers and/or network devices must include a special notice that must state that the system may only be accessed by authorized users, users who logons represent that they are authorized to do so, unauthorized system usage or abuse is subject to criminal prosecution, system usage will be monitored and logged, and by logging into the subject Computer and the Village of Sea Ranch Lakes network, the user has read, understands, and will comply with the Village of Sea Ranch Lakes Information Technology Policies and Procedure Manual.

D. AUDIT LOGS

All production application systems that handle critical Village information must generate logs that capture user-initiated logon attempts (successful or failed), addition, modification, and deletion transactions, user session activity including user IDs, logon date and time, logoff date and time, changes to the privileges of users, and system start-ups and shut-downs if the subject application system is able to produce such audit logs.

E. DATA BACKUPS

All critical business information and critical software resident on Village server systems must be periodically backed-up for recovery purposes. The rotation, recycling of the media used for backups, and the storage location used will be defined by the Village Clerk, as per the business requirements.

.

VII. SECURITY INCIDENT RESPONSE POLICY

A. PURPOSE

This document describes the Village of Sea Ranch Lakes's overall plan for preparing and responding to both physical and electronic information security incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this Security Incident Response Plan is to prepare for, detect, and respond to security incidents. It provides a framework by which the Incident Response Team (IRT) shall determine the scope and risk of an incident, respond appropriately to that incident, communicate the results and risks to all stakeholders, and reduce the likelihood of an incident from occurring or reoccurring.

B. SCOPE

This plan applies to all physical locations, information systems, all Criminal Justice Information (CJI) data, Protected Health Information (PHI) data, Cardholder data, Personally Identifiable Information, any other sensitive data type stored by the Village, networks of the Village of Sea Ranch Lakes, and any person or device that gains access to these systems or data.

C. MAINTAINING CURRENCY

It is the responsibility of the Village Clerk to maintain and revise this policy to ensure that it is always in a ready state.

D. DEFINITIONS

Event: An exception to the normal operation of infrastructure, systems, or services. Not all events become incidents.

Incident: An event that, as assessed by the staff, violates the policies of the Village of Sea Ranch Lakes as related to Information Security, Physical Security, or Acceptable Use; other Village of Sea Ranch Lakes policies, standards, or code of conduct; or threatens the confidentiality, integrity, or availability of information systems or CJI event.

Incidents will be categorized according to their potential for the exposure of protected data or the criticality of the resource, using a four (4) level system of:

0- Low

1- Medium

2 - High

3 - Critical

Incidents can include, but are not limited to:

- Malware/viruses
- Ransomware
- Phishing
- Unauthorized electronic access
- Account compromise
- Breach of information
- Unusual, unexplained, or repeated loss of connectivity
- Unauthorized physical access
- Loss or destruction of physical files, etc.
- Denial of Service

Criminal Justice Information (CJI): As defined in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and by the Florida Department of Law Enforcement.

Protected Health Information (PHI}: The HIPAA Privacy Rule that provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Cardholder Data: As defined by the PCI Security Standards Council (PCI SSC), the body that administers the PCI DSS, defines cardholder data as "At a minimum, cardholder data consists of the **full** PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code [found on the magnetic stripe]. Sensitive Authentication Data are additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction."

E. EVIDENCE PRESERVATION

The goal of any incident response is to reduce and contain the impact of an incident and ensure that information security related assets are returned to service in the timeliest manner possible. The need for a rapid response is balanced by the need to collect and preserve evidence in a manner consistent with state and federal laws, and to abide by legal and administrative requirements for documentation and chain-of-custody.

F. INCIDENT RESPONSE

In accordance with the FBI CJIS Security Policy, based off the National Institute of Standards and Technology (NIST) Special Publication 800-61 rev. 2, the Incident Response Life Cycle consists of a series of phases-distinct sets of activities that will assist in the handling of a security incident, from start to finish.

G. PREPARATION

Preparation includes those activities that enable the Village of Sea Ranch Lakes to respond to an incident. These include a variety of policies, procedures, tools, as well as governance and communications plans.

The Village of Sea Ranch Lakes utilizes several mechanisms to prevent, and prepare to respond to, an incident.

a) Security Awareness Training: The Village of Sea Ranch Lakes requires regular security awareness training provided through KnowBe4. This training covers additional ongoing threats to systems such as malware, phishing, social engineering, ransomware, and other threats as they become known. This training also performs regular phishing campaigns to evaluate the Village's security posture for this attack vector. All personnel with access to CJI data are required to take FBI CJIS Security Policy-compliant Security Awareness Training. This training must be updated at a minimum of every two years.

b) Malware/Antivirus/Spyware Protections: All information system terminals, as well as key information flow points on the network, are protected by continuous defense against malware/antivirus/spyware and other known malicious attacks. These defense mechanisms are kept up to date without the need for end user intervention, and end users are restricted from accessing, modifying, disabling, or making other changes to the defense mechanisms.

c) Firewalls: Multiple firewalls are in place within the network to provide the necessary depth of defense. The Village Clerk keeps all firewalls up to date with the latest security patches and other relevant upgrades, as well as maintains an active backup of the latest security configuration.

d) Personnel Security Measures: All Village staff with access to CJI or those areas in which CJI is accessed, stored, modified, transmitted, or maintained have been cleared to the required Personnel Security standards set forth in FBI CJIS Security Policy section 5.12.1 and FDLE requirements.

e) Physical Security Measures: All locations within the Village of Sea Ranch Lakes that house CJI or CJI-related information systems are secured to the required criteria set forth in FBI CJIS Security Policy section

f) Event Logs: Event logging is maintained at all applicable levels, capturing all the required events and content specified for CJI through FBI CJIS Security Policy sections 5.4.1.1 and 5.4.1.1.1, retained for the specified period, and reviewed weekly.

g) Patching/Updating: Systems shall be patched and updated as new security patches and hot fixes are released. Any software or hardware product that reaches the end of the manufacturers service and support life for patching will be deemed out-of-compliance and replaced.

H. STAFFING

The Village of Sea Ranch Lakes will strive to maintain adequate staff levels and third-party support to investigate each incident to completion and communicate its status to other parties while it continues to monitor the tools that detect new events.

I. TRAINING

No incident response capability can be effectively maintained over time without proper and ongoing training. The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested, and translated into recommendations for enhancements. All pertinent Village staff will be trained on a periodic basis in security awareness, procedures for reporting and handling incidents to ensure a consistent and appropriate response to an incident, and that post-incident findings are incorporated into policy and procedure.

VIII. DETECTION AND ANALYSIS

A. DETECTION

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an incident requires the immediate activation of the IRT as listed in Appendix A. The determination of a security incident can arise from one or several circumstances simultaneously.
Means by which detection can occur include:

a) Trained personnel reviewing collected event data for evidence of compromise.
b) Software applications analyzing events, trends, and patterns of behavior.
c) Intrusion Protection/Intrusion Detection devices alerting to unusual network or port traffic.
d) The observation of suspicious or anomalous activity within a Village of Sea Ranch Lakes facility or on a computer system.

It is critical in this phase:

a) To detect whether a security incident has occurred.
b) To determine the method of attack.
c) To determine the impact of the incident to the mission, systems, and personnel involved in the incident.
d) To obtain or create intelligence products regarding attack modes and methods.

B. ANALYSIS

Analysis of the incident indicators will be performed in a manner consistent with the type of incident. In the event of a physical incident, appropriate steps will be taken to determine weaknesses in either the physical security of the facility, its monitoring tools, or its training programs to assess areas for process improvement or change. For an electronic incident, the Village will utilize, its tools, vendors, and contractors to perform static and dynamic analysis of malicious code within their capability, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced. These analyses can be performed either manually or by utilizing automated tools dependent upon the situation, timeliness, and availability of resources.

C. INCIDENT CATEGORIES

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to The Village of Sea Ranch Lakes and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to the Village's image, or impact to trust by the Village's customers and citizens, etc. The below table provides a listing of the severity levels and a definition of each severity level.

Severity Level	Description
0-Low	Incident where the impact is minimal. Examples may be e-mail SPAM, isolated virus infections, etc.

1- Medium	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, meet the Village's mission, delayed delivery of critical electronic mail or data transfers, etc.
2 - High	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of our mission functions. The Village's proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting over 1 percent of employees, Public Safety systems are unavailable, or the Village's Clerk has been notified.
3 – Critical	Incident where the impact is catastrophic. Examples may be ransomware, denial of service or a shutdown of all the Village's network services due to natural or manmade causes. The Village's proprietary or confidential information has been compromised and published in/on a public venue or site. Public safety systems are unavailable.

D. INCIDENT REPORTING

If an incident involves or is suspected of involving Criminal Justice Information, the Information Security Officer {ISO} will be contacted and provided a CJIS-016 "Information Security Officer (ISO) Security Incident Report" and should work with the Village's agency representatives for CJI compliance.

IX. CONTAINMENT, ERADICATION, AND RECOVERY

A. CONTAINMENT

The Village Clerk is responsible for containment and will document all containment activities during an incident.

Containment activities for security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. This requires intelligence gathered by the detection and analysis phases of the incident - identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

B. ERADICATION

The Village Clerk is responsible for eradication and will document all eradication activities during an incident.

Eradication efforts for a security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created}, identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

C. RECOVERY

The Village Clerk is responsible for recovery and will document all recovery activities during an incident.

Recovery efforts for incidents will involve the restoration of affected systems to normal operation. This is dependent upon the type of incident experienced but may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

D. POST-INCIDENT ACTIVITY

The Village Clerk is responsible for documenting and communicating post-incident activity.

Post-incident activities will occur after the detection, analysis, containment, eradication, and recovery from a security incident. One of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Important items to be reviewed and considered for documentation are:

a) Exactly what happened, and at what times?
b) How well did staff perform in dealing with the incident?
c) What information was needed sooner?
d) Were any steps or actions taken that might have inhibited the recovery?
e) What should be done differently the next time a similar incident occurs?
f) How could information sharing with other organizations have been improved?
g) What corrective actions can prevent similar actions in the future?
h) What precursors or indicators should be watched for in the future to detect similar incidents?
i) What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Post-incident activities will be incorporated into future training opportunities for all parties involved in the incident, from victims to system administration personnel to incident responders.

E. ESCALATION

The escalation process will be initiated to involve other appropriate resources as the incident increases in scope and impact. Incidents should be handled at the lowest escalation level that can respond to the incident with as few resources as possible to reduce the total impact and maintain limits on cyber-incident knowledge. The table below defines the escalation levels with the associated team members involvement.

Severity	Response Team Member Involvement	Description
0- Low	IT Technical Support Staff or vendor	Normal Operations
1-Medium	IT technical support staff or vendor Village Clerk	The Village is aware of a potential or actual threat and is responding to that threat.
2 - High	IT technical support staff or vendor Village Clerk	An obvious threat has impacted business operations. Determine course of action for containment and eradication. Message staff of required actions and operational acts if necessary.

3 – Critical	IT technical support staff or vendor Village Clerk Village Attorney	Threat is widespread with significant impact. Determine course of action for containment, mitigation, and eradication. Message staff and officials. Prepare for legal action. Prepare for a public statement.

X. Data and Asset/Component Sanitization, Destruction, and Disposal

A. Purpose

The purpose of this section is to establish guidelines for the proper sanitization, destruction, and disposal of data and IT assets/components in accordance with NIST standards, specifically NIST Special Publication 800-88 Revision 1, "Guidelines for Media Sanitization."

B. Scope

This policy applies to all employees, contractors, and third parties who handle, manage, or dispose of Village-owned data and IT assets/components.

C. Data Sanitization

a) All data stored on media must be securely erased or sanitized before the media can be reused, transferred, or disposed of.
b) The sanitization method used must be appropriate for the type of media and the sensitivity of the data, as outlined in NIST SP 800-88 Rev. 1.
c) Acceptable sanitization methods include:
- Clear: Overwriting media with non-sensitive data
- Purge: Applying physical or logical techniques to render data recovery infeasible
- Destroy: Physical destruction of media

D. Asset/Component Disposal

a) All IT assets/components must be properly sanitized before disposal to prevent unauthorized access to residual data.
b) The disposal method used must be appropriate for the type of asset/component and the sensitivity of the data it contained.
c) Acceptable disposal methods include:
- Recycling: Sending assets/components to an authorized recycling facility
- Destruction: Physical destruction of assets/components

E. Documentation and Verification

a) All sanitization and disposal activities must be documented, including the date, method used, and the responsible party.
b) Verification of successful sanitization and disposal must be obtained and recorded.

F. . Responsibilities

a) The IT department is responsible for ensuring that all data and assets/components are sanitized and disposed of in accordance with this policy.
b) Employees, contractors, and third parties are responsible for promptly reporting any data or assets/components that require sanitization or disposal to the IT department.

G. Compliance

a) Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
b) Periodic audits will be conducted to ensure compliance with this policy and NIST standards.

By adhering to these guidelines, our organization ensures the secure and responsible handling of data and IT assets/components throughout their lifecycle, m*inimizing the risk of unauthorize*d access to sensitive information.

XI. DISASTER RECOVERY PLAN

A. Purpose and Scope

This Disaster Recovery Plan (DRP) establishes the procedures to recover the Village of Sea Ranch Lakes's critical IT systems, applications, and data in the event of a disruption or disaster. The plan covers all essential infrastructure, including servers, networks, databases, and applications critical to the Village's operations.

B. Roles and Responsibilities

a) Disaster Recovery Coordinator (DRC): The Village Clerk or a designated individual responsible for overseeing the execution of the DRP.
b) IT Department: Responsible for implementing the technical aspects of the DRP, including system recovery and data restoration.

C. Risk Assessment

A comprehensive risk assessment will be conducted monthly to identify potential threats, vulnerabilities, and the impact of disruptions on the Village's critical systems and processes. The assessment will be reviewed and updated as needed.

D. Business Impact Analysis (BIA)

A BIA will be performed annually to identify critical systems, applications, and data, and to establish recovery time objectives (RTOs) and recovery point objectives (RPOs) for each. The BIA will be reviewed and updated as needed.

E. Recovery Strategies

a) Backup and Restore: Critical systems and data will be backed up daily, with backups stored offsite in a secure location. Backups will be tested monthly to ensure data integrity and recoverability.
b) Alternate Processing Site: The Village will maintain a contract with a third-party provider for an alternate processing site in the event of a disaster. The alternate site will be equipped with the necessary hardware, software, and connectivity to support critical operations.
c) Cloud-based Disaster Recovery: Critical applications and data will be replicated to a cloud-based disaster recovery solution, providing an additional layer of redundancy and recoverability.

F. Data Backup and Storage

a) Backup Frequency: Critical systems and data will be backed up daily, with incremental backups performed throughout the day as needed.
b) Backup Retention: Daily backups will be retained for 30 days, weekly backups for 3 months, and monthly backups for 1 year.
c) Offsite Storage: Backup media will be stored offsite in a secure, geographically diverse location.
d) Backup Testing: Backups will be tested monthly to verify data integrity and recoverability.

G. Disaster Recovery Procedures

a) Activation Criteria: The DRP will be activated when a disruption is expected to exceed 4 hours or when deemed necessary by the Disaster Recovery Coordinator.
b) Notification Procedures: The Disaster Recovery Coordinator will notify the Disaster Recovery Team of the DRP activation.
c) Recovery Procedures: Detailed step-by-step recovery procedures will be maintained for each critical system, application, and data set. These procedures will be reviewed and updated annually.

H. Testing and Maintenance

a) Testing Schedule: The DRP will be tested bi-annually, with tabletop exercises, walkthrough drills, and functional tests.
b) Test Results: Test results will be documented, and the DRP will be updated based on lessons learned.

I. Training and Awareness

a) Training: All Disaster Recovery Team members and relevant personnel will receive annual training on their roles and responsibilities during a disaster recovery event.
b) Awareness: Annual awareness programs will be conducted to ensure all staff remain familiar with the DRP and its procedures.

J. Plan Review and Update

The DRP will be reviewed and updated annually or whenever significant changes occur in the Village's IT environment or business processes. The Disaster Recovery Coordinator is responsible for ensuring the plan remains current and effective.

By implementing this comprehensive Disaster Recovery Plan, the Village of Sea Ranch Lakes demonstrates its commitment to ensuring the continuity of its critical operations and the protection of its data and IT assets in the event of a disruption or disaster.