INFORMATION TECHNOLOGY POLICY

SPINZER EQUITIES (PVT) LTD

Contents

Document Review and Approval

Revision History:

Sr.	Version	Author	Date	Revision
1				
2				
3				
4				
5				

Reviewed By:

Sr.	Reviewer	Signature	Date Reviewed
1			
2			
3			
4			
5			

Approved By:

Sr.	Name	Signature	Date Approved
1			
2			
3			
4			
5			

INFORMATION TECHNOLOGY AND SECURITY POLICY

PURPOSE

a) To ensure the efficient, effective, and secure use of information technology (IT) resources.
b) To protect the confidentiality, integrity, and availability of information assets in Spinzer Equities Private Limited.
c) To ensure adherence to and compliance with company policies.
d) To maintain the security and confidentiality of passwords
e) To control and manage access rights to company systems
f) To ensure the physical security of critical IT infrastructure
g) To manage the use of removable storage media and prevent data loss.
h) To ensure the safety of employees during emergencies
i) To maintain the security and functionality of software through timely patching
j) To manage and mitigate information security risks associated with outsourcing activities
k) To effectively manage and respond to information security incidents.

SCOPE

a) **Compliance Requirement:** To adhere to minimum standards for software and applications.
b) **Software/Applications Scope:** Includes order management, front and back office, internet-based trading systems, and related software, whether used directly, indirectly, or outsourced.
c) **Operational Coverage:** Pertains to customer onboarding, trading, risk management, clearing, settlement, and maintenance of books and accounts.
d) **Testing and Certification:** Mandates regular testing and certification of relevant software and applications.
e) **Supplier Management Standards:** Establishes requirements for managing suppliers/vendors.
f) **Cloud Services:** Includes standards related to the use of cloud services.
g) **Incident Management:** Specifies procedures for handling security breaches.
h) **Broad Applicability:** Applicable to BODs, all employees, suppliers/vendors, and all associated software and applications.

RESPONSIBILITIES OF THE BODS AND OVERSIGHT MECHANISM FOR POLICY ADHERENCE

The Board is responsible to:

(a) Formulate and communicate a comprehensive IT & security policy ("Policy") meeting or exceeding the Minimum Information Security Standards prescribed by the Pakistan Stock Exchange Limited (PSX) for adoption and compliance by the Securities Brokers.
(b) Review, approve, and oversee Policy implementation.
(c) Approve supplier engagement criteria/procedures, defining staff roles in outsourcing.
(d) Allocate sufficient resources for timely security measure implementation per the approved Policy.
(e) Implement and regularly review effective technology risk management, including

timely risk identification, assessment, mitigation, monitoring, and reporting.
(f) Implement an adequate oversight mechanism for strict Policy adherence.
(g) Review and approve key decisions on critical information security issues.
(h) Conduct regular awareness and training sessions for all employees.

The following procedures will be employed by the BOD for designing, implementing, and monitoring the policy.

(a) Policy Formulation and Communication:

- **Procedure:**
    - Establish a cross-functional team to draft the Policy.
    - Conduct risk assessments and align the Policy with industry standards.
    - Engage relevant stakeholders for feedback and approval.
    - Disseminate the Policy through multiple channels (email, intranet, training sessions).
    - Obtain signed acknowledgments of receipt from employees.

(b) Policy Review, Approval, and Oversight:

- **Procedure:**
    - Assign a designated committee or manager for Policy review and approval.
    - Establish a formal approval process with clear timelines and documentation.
    - Conduct regular audits and compliance checks to assess Policy adherence.
    - Address non-compliance through corrective actions and disciplinary measures, if needed.

(c) Supplier Engagement Criteria and Procedures:

- **Procedure:**
    - Develop a supplier assessment framework with security-related criteria.
    - Define roles and responsibilities for staff involved in supplier selection and onboarding.
    - Embed security requirements in contracts and service level agreements (SLAs).
    - Conduct regular security audits of third-party providers.

(d) Resource Allocation:

- **Procedure:**
    - Conduct a cost-benefit analysis of security measures.
    - Prioritize resource allocation based on risk assessment and Policy requirements.
    - Establish a budget for security-related expenses.
    - Track resource utilization and adjust as needed.

(e) Technology Risk Management:

- **Procedure:**

- Implement a risk management framework aligned with the Policy.
- Conduct regular risk assessments to identify potential threats and vulnerabilities.
- Prioritize and implement risk mitigation controls.
- Monitor risks and control effectiveness through continuous monitoring tools.
- Generate periodic risk reports for management review.

(f) Oversight Mechanism:

- **Procedure:**
  - Appoint a dedicated team or individual for oversight responsibility.
  - Establish monitoring and reporting procedures to track Policy compliance.
  - Conduct regular audits and assessments of security controls.
  - Investigate and address incidents of non-compliance.

(g) Key Decision Review and Approval:

- **Procedure:**
  - Define a clear decision-making process for critical information security issues.
  - Involve relevant stakeholders in decision-making, including senior management.
  - Document decisions and rationale for future reference.

(h) Awareness and Training:

- **Procedure:**
  - Develop a comprehensive training program covering Policy content and security best practices.
  - Deliver training to all employees at appropriate intervals.
  - Track training completion and effectiveness through assessments.
  - Offer ongoing awareness campaigns and resources.

ACCESS CONTROLS STANDARDS AND PROCEDURES

All computer systems shall have a log-on authentication procedure including at-least a unique user ID & password.

1- User Access Controls

(a) Unique, Identifiable User IDs:

- **Procedure:**
  - Establish a user ID creation process with clear guidelines.
  - Use recognizable patterns (e.g., firstname.lastname) or a dedicated ID generator.
  - Integrate ID management with HR systems for consistency.

(b) Hidden Application Identifiers:

- **Procedure:**
    - Configure applications to conceal identifiers until successful login.
    - Test for potential vulnerabilities that might reveal identifiers prematurely.

(c) No Help Messages During Login:

- **Procedure:**
    - Disable any built-in help features during login screens.
    - Provide alternative support channels (e.g., password reset links).

(d) Full Data Validation and Error Handling:

- **Procedure:**
    - Modify login logic to validate all input fields together.
    - Implement generic error messages for failed login attempts.

(e) Brute Force Protection:

- **Procedure:**
    - Set limits on consecutive incorrect login attempts (e.g., 3-5).
    - Implement account lockout mechanisms for exceeded limits.
    - Consider CAPTCHA or similar challenges for further protection.

(f) Inactive Session Lockout:

- **Procedure:**
    - Configure session timeouts to lock screens after 15 minutes (or less).
    - Use screensavers with password protection for visual security.

(g) Multi-Factor Authentication (MFA) for Critical Systems:

- **Procedure:**
    - Evaluate and select an appropriate MFA solution.
    - Integrate it with critical systems and user accounts.
    - Provide clear setup and usage instructions to users.

(h) Forced Password Change on First Login:

- **Procedure:**
    - Configure applications to mandate password changes upon initial login.
    - Enforce strong password policies (e.g., complexity, length, expiration).

(i) Need-to-Know Access Controls:

- **Procedure:**
    - Conduct thorough access control assessments.

- Grant access permissions based on job roles and responsibilities.
- Conduct regular reviews and audits to ensure compliance.

(j) Authorized Access with Strong Authentication:

- **Procedure:**
  - Establish a formal process for requesting and approving access.
  - Implement robust authentication methods (e.g., tokens, biometrics).
  - Regularly review and revoke access when no longer needed.

(k) Strict Supervision and Monitoring:

- **Procedure:**
  - Implement tools for logging and monitoring user activity.
  - Conduct regular access reviews and audits.
  - Enforce disciplinary actions for policy violations.

2- Password Management

The application should provide capability to enforce password control including complexity, expiration, account lockout and re-use time.

(a) Mandatory User Authentication:

- **Procedure:**
  - Configure applications to require user ID and password for access.
  - Integrate with authentication systems (e.g., Active Directory).
  - Disable any alternative login methods (e.g., guest access).

(b) Access Control:

(i) Program applications for password validation:

- **Procedure:**
  - Program applications to validate passwords against unique usernames before granting access.
  - Enforce access control lists (ACLs) to restrict unauthorized access.

(ii) Confirmation Procedure:

- **Procedure:**
  - Implement password re-entry fields for error correction.
  - Display password complexity requirements during creation.

(iii) Password Complexity:

- **Procedure:**

- Set minimum password length requirements.
- Enforce character diversity rules (uppercase, lowercase, numbers, special characters).
- Use password strength meters for visual guidance.

(iv) Regular Password Changes:

- **Procedure:**
  - Configure password expiration reminders and forced resets after 120 days.
  - Maintain password history to prevent reuse within the past 3 changes.

(v) Failed Login Attempts:

- **Procedure:**
  - Implement account lockout mechanisms after 5 failed attempts.
  - Configure unlock options (admin reset or automatic unlock after 30 minutes).

(vi) Customer-Facing App Lockout:

- **Procedure:**
  - Activate account lockout after 5 failed logins.
  - Establish reset procedures using secure email links, OTP SMS, or manual broker verification.

(vii) Initial Passwords:

- **Procedure:**
  - Generate unique initial passwords for each new user.
  - Mandate password changes upon first login.

(viii) No Clear Text Passwords:

- **Procedure:**
  - Mask passwords with asterisks or dots on screens.
  - Disable password printing functionality.
  - Configure applications to avoid password caching.

(ix) Password Encryption:

- **Procedure:**
  - Use secure protocols (e.g., HTTPS, SSL/TLS) for password transmission.
  - Enforce strong encryption algorithms for password storage.

(x) Secure Password Storage:

- **Procedure:**
  - Utilize password hashing techniques (e.g., bcrypt, scrypt) for storage.

- Avoid storing passwords in plain text within systems, devices, files, or logs.
- Clear password-related memory after processing.

(xi) Monitoring:

- **Procedure:**
  - Implement tools to log and alert on multiple failed login attempts.
  - Set alerts for login attempts outside regular working hours.

(xii) Annual Access Review:

- **Procedure:**
  - Conduct regular reviews of user access privileges.
  - Revoke access for terminated or inactive users.
  - Update access permissions based on role changes.

3- User Administration

a) Unique Admin IDs:

- **Policy:** Use identifiable, named user IDs for security administrators (no shared/group IDs unless documented and approved for business needs).
- **Procedure:** Implement mandatory unique IDs in systems, integrate with user management systems.

b) Access Control Segregation:

- **Policy:** Separate access management roles to prevent unauthorized changes:
  - **Request:** User initiates access request.
  - **Approval:** Authorized personnel review and approve requests.
  - **Implementation:** Separate individual implements authorized requests.
  - **Monitoring:** Monitor access changes for anomalies.
- **Procedure:** Designate distinct roles for each function, enforce approvals and review processes.

c) Granular User Access:

- **Policy:** Configure user access with sufficient detail to maintain data confidentiality, integrity, and segregation of duties.
- **Procedure:** Implement granular access controls within systems, assign permissions based on specific needs.

d) Compensating Controls:

- **Policy:** If granular access controls aren't available, implement compensating controls to mitigate risks.

- **Procedure:** Identify limitations, implement alternative measures like dual approvals or activity monitoring.

e) Separate Privileged Access:

- **Policy:** Assign privileged access rights to dedicated IDs, avoid using them for regular activities.
- **Procedure:** Implement separate privileged accounts for specific tasks, enforce usage restrictions.

f) Maker/Checker User Administration:

- **Policy:** Support access control segregation with a dedicated user administration interface with separate roles for requestors and approvers.
- **Procedure:** Configure systems with maker/checker functionality for access requests and changes.

g) User Deactivation:

- **Policy:** Upon employee departure or access revocation, deactivate user privileges on their last working day.
- **Procedure:** Integrate user management with HR systems, automate privilege removal based on employment status.

h) Detailed Logging:

- **Policy:** The application must create detailed logs for all mentioned access control activities.
- **Procedure:** Configure systems to log user actions, access changes, and audit trails.

i) Privileged User Review:

- **Policy:** Review privileged user access rights at least quarterly.
- **Procedure:** Schedule regular reviews of privileged accounts, assess continued need and adjust permissions.

j) Off-Hours Login Monitoring:

- **Policy:** Implement a mechanism to detect and alert on login attempts outside of regular office hours.
- **Procedure:** Configure systems to monitor login activity, trigger alerts for suspicious attempts.

k) Access Report Generation:

- **Policy:** Provide functionality to generate the following on-demand reports:
    - User Access Summary Report
    - User Access Detailed Report
    - Information Security Administrator Detailed Report

- **Procedure:** Develop reporting tools within the application to provide these reports with relevant data.

DATA SECURITY STANDARDS AND PROCEDURES

a) Always Encrypt Critical Data:

- **Policy:** All critical data must be stored in an encrypted form regardless of medium, mechanism, or format.
- **Procedure:** Implement encryption methods for data at rest (e.g., databases, filesystems) using strong algorithms and key management practices.

b) Always Encrypt Data Transmission:

- **Policy:** All critical data transmissions between any two nodes (internal or external) must be encrypted regardless of mechanism or format.
- **Procedure:** Configure secure communication protocols (e.g., HTTPS, TLS/SSL) for network traffic and application-level encryption for sensitive data transfers.

c) Secure Peripheral Devices:

- **Policy:** Information security policies apply to devices like mobile phones, faxes, printers, scanners, etc., that handle sensitive data.
- **Procedure:** Define access controls for personnel, restrict network connectivity, implement data capture security measures (e.g., password protection, encryption).

d) Strict Data Access Controls:

- **Policy:** Implement strict data access controls for all personnel, including privileged users like system administrators and developers.
- **Procedure:** Minimize direct access to critical data, monitor and log access activities, enforce strong authentication and authorization, implement least privilege principle.

e) Secure Backups and Retention:

- **Policy:** Ensure adequate backups of critical data according to retention policies, and secure backup locations.
- **Procedure:** Automate backups based on data sensitivity and retention requirements, store backups in secure locations separate from primary systems, implement access controls and encryption for backups.

Key Points:

- Emphasis on **comprehensive encryption** for data at rest and in transit.
- **Strict access controls** regardless of user roles or privileges.
- **Secure peripheral devices** handling sensitive data.
- **Regular backups and secure storage** for critical data.

POLICY AND PROCEDURE FOR SECURING PERIMETER OF CRITICAL

EQUIPMENT ROOM

(a) Security Perimeters

- **Policy:** Establish security perimeters to safeguard areas with information systems against unauthorized access, damage, and interference.
- **Procedure**: Define secure areas, implement physical barriers, and control access points. Regularly inspect and maintain these perimeters.

(b) Monitoring Physical Access

- **Policy:** Continuously monitor physical access to information systems to identify and react to security incidents.
- **Procedure**: Install surveillance systems, maintain access logs, and regularly review access records. Implement an incident response protocol for anomalies.

(c) Protection from Power Failures

- **Policy:** Shield information systems from disruptions due to power outages and utility failures.
- **Procedure**: Install uninterruptible power supplies (UPS) and backup generators. Conduct regular maintenance and testing of these systems.

(d) Restricting Physical Access

- **Policy:** Limit physical access to critical systems to authorized personnel only. Supervise access of outsourced staff and visitors.
- **Procedure**: Implement access control mechanisms, maintain an access authorization list, and ensure constant supervision of external personnel in sensitive areas.

(e) Revoking Access

- **Policy:** Immediately revoke physical access to critical systems when it is no longer required.
- **Procedure**: Regularly review access rights and promptly deactivate access for individuals whose authorization has expired or is no longer needed.

(f) Securing Critical Equipment Room

- **Policy:** Secure the perimeter of critical equipment rooms with physical, human, and procedural controls.
- **Procedure**: Employ CCTVs, card access systems, and security personnel. Conduct regular security audits and maintain access control logs.

(g) Removable Storage Media

- **Policy:** Restrict access to removable storage media to authorized personnel and protect it against physical and environmental harm.
- **Procedure**: Enforce encryption and password protection for data on removable media. Log and monitor the movement of these assets and ensure secure off-site transportation only with prior authorization.

(h) Secure Disposal or Re-Use of Equipment

- **Policy:** Ensure secure disposal or reuse of equipment containing storage media.
- **Procedure**: Use data destruction methods like formatting, physical destruction, or overwriting to render data non-retrievable. Maintain disposal records and adhere to data-disposal and retention standards.

(i) Emergency Procedures

- **Policy:** Document and disseminate emergency and evacuation procedures, testing them annually.
- **Procedure**: Create comprehensive emergency plans, conduct regular drills, and update procedures based on test outcomes. Ensure all personnel are familiar with these procedures.

PATCH MANAGEMENT STANDARDS AND PROCEDURES

(a) Patch Management Procedures

- **Summary**: Implement procedures for identifying, categorizing, and prioritizing security patches and updates, with established timeframes for implementation.
- **Procedure**: Regularly scan for new patches, classify them based on severity and impact, and assign implementation deadlines. Ensure patches are applied within these timeframes.

(b) Testing of Security Patches

- **Summary**: Conduct thorough testing of security patches and updates in a non-production environment to ensure they do not adversely affect other systems.
- **Procedure**: Set up a test environment mirroring the production setup. Apply and evaluate patches here first to check for system compatibility and unintended consequences.

(c) Adherence to Change Management Process

- **Summary**: Rigorously follow the Change Management Process, documenting all changes caused by patch application to track and manage potential issues.
- **Procedure**: Document each step of the patching process, including system status before and after the patch. Monitor and record system responses and anomalies post-patching.

(d) Automatic Patching and Updates

- **Summary**: Where justifiable and feasible, enable automatic patching and updates for operating systems and software to maintain up-to-date security controls.
- **Procedure**: Activate automatic update features in software settings, ensuring justification for this approach is recorded. Regularly review and audit the effectiveness of automatic updates.

SUPPLIER MANAGEMENT STANDARDS AND ADDRESSING INFORMATION SECURITY RISKS IN OUTSOURCING ACTIVITIES

(a) Outsourcing Activities Security

- **Summary**: Establish policies and procedures to manage information security risks in outsourcing activities like data center operations and cloud computing services.
- **Procedure**: Assess security risks for each outsourced activity, define security requirements, and ensure compliance through regular audits.

(b) Supplier Engagement Procedures

- **Summary**: Define and communicate procedures for supplier selection and engagement, including approval authorities.
- **Procedure**: Develop a structured supplier selection process, establish criteria for evaluation, and assign roles for approvals.

(c) Reporting to the Board

- **Summary**: Report details of engaged suppliers and corresponding Service Level Agreements (SLAs) to the Board.
- **Procedure**: Maintain records of all supplier contracts and SLAs, and present regular reports to the Board for oversight.

(d) Integrity Controls

- **Summary**: Implement controls to ensure the integrity of information processing by suppliers.
- **Procedure**: Establish verification mechanisms for data integrity, conduct regular checks, and mandate supplier compliance with data integrity standards.

(e) Recovery and Contingency Arrangements

- **Summary**: Ensure recovery and contingency plans are in place for uninterrupted information processing by suppliers.
- **Procedure**: Define recovery time objectives, ensure suppliers have robust contingency plans, and conduct periodic testing.

(f) Supplier Background Review

- **Summary**: Conduct thorough background checks of suppliers, especially Cloud Service Providers, considering various risk factors.
- **Procedure**: Evaluate suppliers based on experience, track record, financial strength, and compliance. Perform due diligence for CSPs including physical security and internal controls.

(g) Service Level Agreement (SLA)

- **Summary**: Execute a legally vetted SLA with suppliers, covering control implementation, incident management, business continuity, and security compliance.
- **Procedure**: Draft SLAs with detailed terms, get legal vetting, and ensure mutual agreement on all aspects including performance and security controls.

(h) Avoiding Lock-In Clauses

- **Summary**: Refrain from including lock-in clauses or exclusivity arrangements in SLAs.
- **Procedure**: Negotiate SLAs to avoid restrictive clauses, ensuring flexibility and adaptability in supplier relationships.

(i) Termination Rights

- **Summary**: Secure the right to terminate the SLA under severe circumstances affecting information security.
- **Procedure**: Include termination clauses in SLAs that allow for exit in case of security compromises or significant risks.

(j) Confidentiality Agreements

- **Summary**: Sign confidentiality and Non-Disclosure Agreements before executing SLAs.
- **Procedure**: Draft and mutually agree on non-disclosure terms to protect sensitive information before formalizing SLAs.

(k) Service Performance Monitoring

- **Summary**: Regularly monitor and review supplier service performance against SLA terms.

- **Procedure**: Establish monitoring processes, conduct periodic reviews, and enforce SLA compliance.

(l) PSX Approval for Cloud Arrangements

- **Summary**: Obtain prior approval from PSX before entering into cloud arrangements.
- **Procedure**: Submit proposed cloud arrangements to PSX for approval, ensuring compliance with relevant regulations and guidelines.

(m) Restrictions on Core Trading Applications

- **Summary**: Prohibit cloud-based outsourcing for core trading applications, services, operations, and business processes handling investor/trading data.
- **Procedure**: Maintain critical trading systems and data storage in-house or through non-cloud-based solutions.

(n) PSX Prescribed Vendor Criteria

- **Summary**: Comply with PSX-prescribed eligibility criteria for vendors, particularly for brokers' back-office systems.
- **Procedure**: Stay informed about PSX guidelines for vendors, ensure vendor compliance with these criteria before engagement.

INCIDENT MANAGEMENT STANDARDS AND PROCEDURES

(a) Incident Reporting Policies

- **Summary**: Formulate policies and procedures for reporting suspected or actual information security incidents internally to the Board and Senior Management, and externally to PSX and customers if appropriate.
- **Procedure**: Develop a reporting protocol, including escalation channels and communication templates. Train staff on the procedure and ensure timely reporting of incidents.

(b) Employee Awareness

- **Summary**: Ensure all employees and contractors are aware of their responsibility to report any information security events.
- **Procedure**: Include incident reporting responsibilities in employee training programs. Regularly remind and update staff about these responsibilities.

(c) Incident Log Maintenance

- **Summary**: Keep logs of all incidents centrally, accessible only to authorized personnel.
- **Procedure**: Establish a secure, centralized incident logging system. Restrict access to authorized individuals and maintain confidentiality.

(d) Investigation of Alerts

- **Summary**: Investigate alerts from monitoring and detection systems to prevent the expansion, mitigate the effect, and eradicate cyber-attacks or breaches.
- **Procedure**: Set up a protocol for responding to alerts, including initial assessment, containment strategies, and escalation processes.

(e) Incident Log Content

- **Summary**: The incident log must include specific details such as the time, nature, identification method, reporter, extent, priority, and actions taken regarding the incident.

- **Procedure**: Ensure all incident reports are comprehensive, containing all required elements. Train staff on effective incident documentation.

(f) Reporting to PSX

- **Summary**: Promptly report all security incidents and breaches to PSX, including a summary analysis, causes, and resolution steps.
- **Procedure**: Develop a standardized reporting format for PSX notifications. Ensure rapid analysis and reporting post-incident.

(g) Log and Data Preservation

- **Summary**: Preserve logs and data of identified and reported incidents for a period of 3 years or as prescribed by PSX.
- **Procedure**: Implement data retention policies and systems to securely store incident logs and relevant data for the required duration.

(h) Analysis and Improvement

- **Summary**: Analyze incidents of data or system loss or destruction and incorporate lessons learned to strengthen security mechanisms and improve recovery planning.
- **Procedure**: Conduct post-incident reviews to identify weaknesses and areas for improvement. Update security policies and recovery plans based on these insights.

BUSINESS CONTINUITY PLAN (BCP) AND DISASTER RECOVERY (DR) STANDARDS

(a) Compliance with PSX Regulations

- **Summary**: Adhere to clauses 4.27 and 8.3.2 of PSX Regulations as specified by PSX.
- **Procedure**: Regularly review PSX Regulations, ensure all operations and practices align with the specified clauses, and make necessary adjustments to maintain compliance.

(b) Business Continuity Plan (BCP) and Disaster Recovery (DR)

- **Summary**: Implement a BCP and DR to maintain data and transaction integrity.
- **Procedure**: Develop comprehensive BCP and DR plans addressing data backup, system recovery, and transaction integrity preservation in case of disruptions.

(c) Business Impact Analysis for BCP and DR

- **Summary**: Conduct business impact analysis to identify key business activities and operational functions for BCP and DR.
- **Procedure**: Perform a detailed analysis to determine critical business functions and support systems, assessing their impact on operations in the event of disruption.

(d) Resource Identification in BCP and DR

- **Summary**: Clearly document computing resources and office facilities needed for critical business functions in BCP and DR.
- **Procedure**: Identify and list all essential computing resources and facilities. Include detailed resource requirements in BCP and DR documentation.

(e) Documentation of Third-Party Services

- **Summary**: Formally define and document services provided by third parties in a Supplier Agreement.

- **Procedure**: Draft comprehensive agreements with third-party service providers detailing their roles and responsibilities, particularly in the context of BCP and DR.

(f) Periodic BCP Drills

- **Summary**: Regularly conduct drills to validate the effectiveness of the business continuity plan.
- **Procedure**: Schedule and execute periodic drills to test and refine BCP protocols, making adjustments based on outcomes and lessons learned.

(g) BCP/DR Employee Training

- **Summary**: Train employees in BCP/DR procedures, including backup personnel.
- **Procedure**: Develop training programs for BCP/DR, ensure widespread employee participation, and train additional personnel for backup roles.

(h) Annual BCP and DR Review

- **Summary**: Keep the BCP and DR up-to-date with annual reviews and management sign-off.
- **Procedure**: Conduct yearly audits of BCP and DR plans, update them as necessary, and obtain formal approval from management.

(i) Integration of DR and BCP

- **Summary**: Seamlessly integrate the disaster recovery plan with the business continuity plan.
- **Procedure**: Ensure that the DR plan complements and is an integral part of the BCP, with coordinated objectives and procedures.

GENERAL PROVISIONS

- All policies are subject to regular review and updates.
- All employees are required to acknowledge and adhere to these policies.
- Violations of these policies may result in disciplinary action.