TechInnovate Inc. – Strengthening Cybersecurity Resilience

Security Strategy Engineering

Jahvin Bridge

Brendan Ancheta **CYBR-10007**

Lance Santos **Emilija Jasnic**

PASSWORD POLICY

1. **Password Standards for Creation & Complexity**

    1.1 **Password minimum length requirement**: All passwords must have a minimum of 12 characters, 16 characters being the minimum for administrative accounts.

    1.2 **Passwords' Composition of Characters**: All passwords must include a mixture of three to four types of characters (lowercase, uppercase, special characters, numbers).

    1.3 **Password Elements that are Prohibited:** There are no circumstances where dictionary words, staff's personal information, an pattern of characters, or sequential characters will be permitted.

    1.4 **Preferential Usage of Passphrases**: Additional credit for complexity will be granted to passwords that are comprised of random words combinations.

2. **Managing the Lifecycle of Passwords**

    2.1 **Initial Password Creation**: All TechInnovate passwords must be created with a secure process of enrollment via an out of band delivery method for credentials.

    2.2 **Frequent Expiration of Passwords**: All TechInnovate passwords are subject to an expiration period of ninety days, administrative passwords are subject to an expiration period of 60 days.

    2.3 **Triggers to Change Passwords**: TechInnovate passwords will be subject to change following compromise, access attempts by unauthorized users, or a security incident.

    2.4 **Retroactive Password Restrictions**: TechInnovate users can under no circumstance reinstate any of their prior twelve passwords.

3. **Requirements for Password Protection and Storage**

    3.1 **Standards for Hashing Passwords**: TechInnovate passwords are to be encrypted via methods that are industry-standard (i.e., Argon2, Bcrypt, etc.)

    3.2 **Implementation of Password Salting**: Mandatory salt values will accompany each of the unique password hashes, mitigating password spraying, or rainbow table attacks.

    3.3 **Secure Transmission of Passwords**: TechInnovate passwords are to be solely transmitted over encrypted mediums via TLS 1.3 protocols.

3.4 **Segregating Passwords in Storage**: TechInnovate must keep password databases isolated from application databases and stored on a hardened and separate system.

4. **Implementation of Multi-Factor Authentication**

4.1 **Critical TechInnovate Systems**: A system that handles client information, administrative functionality, or financial data requires multi-factor authentication.

Deployment Timeframes

4.1.1 **MFA Implementation in Core TechInnovate Systems**: 45 days

4.1.2 **MFA Implementation in Legacy Systems**: 120 days

4.2 **Acceptable Methods of Authentication**: The permitted methods of authentication are biometric methods on Windows Hello for Business, hardware authentication tokens, and the Microsoft Authenticator App.

4.3 **TechInnovate Protocol for Recovering a Password**: Users may recover their passwords in a documented emergency procedure by providing verification of identity.

5. Auditing Users' Login Activity

5.1 **Monitoring Users' Failed Login Attempts for Sing-In Risk**: TechInnovate IAM system will create a log and alert IT for four failed authentication attempts.

5.2 **Analyzing Users' Behaviour Patterns**: Analysis of users' patterns of authentication will be conducted to track anomalous behaviour such as login locations, times of login, and devices being used to login.

5.3 **Protecting Users' Credentials From Credential Stuffing**: TechInnovate will implement an authentication-attempt rate limit, and utilize CAPTCHA to mitigate automated credential threats.

5.4 **Consistent Auditing of Credentials**: TechInnovate will conduct a monthly audit of users' passwords for compliance verification purposes, combatting against weak password combinations, and to maintain a secure IAM database posture.

ACCESS CONTROL POLICY

1. Implementation of RBAC

1.1 **Definition of Users' Roles**: All the staff positions will be efficiently mapped to a distinct access role, each role will be given clear definitions that contain core information including system permissions, authorization of operations, and requirements for accessing company data.

1.2 **Escalation of Users' Privileges**: A formal process of authorization is required for granting administrative access to a user. All instances of privilege escalation will have a detailed documentation of approval and a defined measure of the temporary time limit.

1.3 **Mitigating Cross-Role Conflicts**: Any combination of roles granted to a user which creates security conflict will be prevented through enforcement of TechInnovate's conditional access policy providing the user restricted access.

1.4 **Permission Reviews**: All TechInnovate users' access permission will be reviewed every 120 days, reduction of privileges will be automated for roles that no longer require an elevated level of system access.

2. Mapping Access & Classifying Information

2.1 **Proper Classification of Data**: TechInnovate data will be properly classified (restricted, confidential, internal, public), with data classification governing level of access protocols.

2.2 **Matrix of User Access**: A thorough matrix will govern each role's access to a specified classification level of data (restricted, confidential, internal, public), business operational capabilities, and TechInnovate business functions.

2.3 **DLP & Content Filtering**: A comprehensive system of content filtering and DLP infrastructure will mitigate unauthorized distribution of data, irrespective of users' authorization level.

2.4 **Vendors & Third-Party**: A separate set of IAM controls will be in place for contractors, clients, and third-parties, containing a distinct set of requirements for authorization and authentication.

3. Managing Various Devices and Identities

3.1 **Detailed Inventory System**: Company-owned or personally owned devices that access TechInnovate resources are registered and managed in the centralized inventory database.

3.2 **Implementation of Federation**: SSO will be put in place to curate a united management of identities throughout all TechInnovate platforms.

3.3 **PKI Protocols**: PKI will be implemented to authenticate company devices, also using PKI controls for granting access to TechInnovate's sensitive databases and systems.

3.4 **Conditional Access**: An extra layer of authentication may be required for a user based on their location, behaviour patterns, or characteristics of their device.

4. Implementing MDM

4.1 **Enrolling Devices into MDM**: All TechInnovate staff's personal devices access

the company's resources will be enrolled in the MDM database, granting TechInnovate proper data protection posture, monitoring end-user devices remotely, and enforcing the company's security policy.

4.2 **Monitoring Mobile Device Compliance**: TechInnovate will monitor the security posture of personal devices, including details such as the version of the operating system, recent application updates, and compliance level for security configuration.

4.3 **Segregation of Application Data**: TechInnovate will implement a system that segregates application data using separate containers for business data and personal data, mitigating risks of cross-contamination of data, and securing the privacy of the end user.

4.4 **Wiping Devices Remotely**: TechInnovate will have the capability to selectively and completely wipe a device remotely for situations where a device has been compromised, reported lost, or is unauthorized for access to company resources.

5. Maintaining Compliance by Auditing

5.1 **Logs of User Access History**: Logging of a user's access incident and events will be comprehensive. These logs will contain information regarding authentication successes and failures, user's authorization history and privilege escalations, as well as a history of the user's access to corporate resources.

5.2 **Tracking and Detecting User Violations**: Users' activities will be monitored via an automated violation detection system which sends real-time violation alerts including violation of policies, abuse of privilege, and unauthorized attempts to access corporate resources.

5.3 **Consistent Behavioral Database Audits**: Every 120 days an audit will be conducted and will comprehensively review TechInnovate users' permissions, history of privileged access, and users' compliance with TechInnovate policies.

5.4 **Responding to Security Incidents**: Access controls will be monitored via playbooks for incident responses, orchestrating a quick containment process, and remediation process for security incidents.

REMOTE WORK POLICY

1. Requirements for VPN

1.1 **VPN Mandate for Staff**: Every connection made to TechInnovate resources remotely must happen through a VPN approved by the organization, under no circumstance will an exception be made for technical limitations or personal convenience of the end user.

1.2 **Standards for Encrypting Data**: All implementations of VPN usage must use industry-standard encryption methods (i.e., AES-256, SHA 256), for all VPN sessions.

1.3 **VPN Integration With IAM**: All VPN implementations must be properly integrated with TechInnovate IAM systems, prompting for MFA before beginning a VPN session, and be aligned with TechInnovate RBAC.

1.4 **Proper Segmentation of Network Traffic**: Industry-standard VPN solutions provide network segmentation capabilities, which prevent a threat actor from having lateral movement between TechInnovate platforms, while simultaneously hardening authorized business communication on the network.

2. Controls to Maintain Network Security

2.1 **Employees' Hardened Network Security**: While working from home, all employees must uphold TechInnovate's standards of security, which includes having WPA3 enabled on wireless network connections, 15 character passwords for routers, and an updated firmware.

2.2 **Avoiding Usage of Public Networks**: All employees are prohibited from accessing corporate resources while on a publicly accessible wireless network, implementing usage of VPN alone is not sufficient for accessing proprietary data.

2.3 **Cellular Data Requirements**: Employees' smartphones must be configured for VPN connections while remotely accessing corporate resources, all usage of public Wi-Fi on a cellular device while accessing corporate resources are prohibited.

2.4 **Proper Monitoring of Home Network**: Employees are responsible for implementing a network-monitoring solution that is capable of detecting an unauthorized network access attempt, and detecting abnormal traffic patterns, properly upholding TechInnovate security policy.

3. Requirements for Device Security

3.1 **Standard for TechInnovate Devices**: Any device that accesses the organization's network remotely must have the minimum security standards of automatically locking screens, and a fully encrypted disk, and have the most recent security updates applied.

3.2 **Proper Endpoint Protection and Management**: Any device remotely connected to the organization's network must have an up to date antivirus and antimalware, and be compliant with the organization's IPS/IDS systems.

3.3 **Security Updates and Management of Patches**: Patches are automated for TechInnovate devices, as well as personal devices, to ensure that all endpoint devices maintain security posture.

4. Accessing the Cloud

4.1 **Implementing SSO**: TechInnovate services have integration of SSO, giving TechInnovate capability of managing authentication and authorization centrally.

4.3 **MFA and Management of Privileged Access**: TechInnovate will implement a MFA system with the Microsoft Authenticator App, and control users' privilege access for administrative functions in the cloud.

4.4 **Proper Cloud Backups**: TechInnovate will implement a cloud-hosted backup system with high-redundancy for recovery purposes and business continuity development.

INCIDENT RESPONSE PLAN

1. Incident Response Team (IRT)

1.1. Establish Roles and Responsibilities: Every member on the IRT should clearly understand the role and duties they must fulfill as a member of the team. It is up to the individual to inquire further and raise attention should there be ambiguity on their role and responsibilities.

1.2. Available 24/7: The IRT should also be available in a functioning capacity in order to be able to respond to any incoming incident at any time.

1.3. Enforce Proper Logging of Incidents: The team should record and log incident processes in a proper manner. This allows for effective analysis of what occurred during the incident, which can then be applied to future events and training

2. Incident Detection

2.1. **Employ Effective Detection Tools:** It is the expectation that there are proper systems in place for detecting and alerting the company to potential anomalies and/or suspicious activity across the company's network.

2.2. **Detection Monitoring:** It is up to the IRT to dedicate an individual(s) to keeping up with alerts received from the monitoring system, and then effectively reporting the information received to relevant parties of the alert.

3. **Incident Response Measures**

3.1. **Downtime Acceptance:** All staff should be prepared to lose access to their devices and/or network, provided the IRT gives effective warning and reason for the loss of access. The IRT should make the best effort in quickly and effectively restoring access to affected users in an incident.

3.2. **Potential Measures Taken:** Staff should be prepared for any of the following actions to be taken in an incident: seizure and containment of their device, disabling of their account, and loss of access to the network. It should be noted this list only covers common actions taken and is not limited to what is stated here.

PHISHING AWARENESS AND TRAINING POLICY

1. **Training Requirements**

1.1. **Training Expectations:** It is mandatory for all staff to undergo Phishing Awareness Training that will be provided by the company. Failure to do so can result in suspensions or even termination of employment if training is not completed within at least a 2 month period after having received notification of it.

1.2. **Results of Training:** If an employee is unable to meet a passing score on the training exercises, they will be expected to undergo training until they are able to do so. Continuous failures of training by an employee will put them under review, where it will be discussed what the best actions moving forward for them will be.

1.3. **Review Training Statistics:** Results of training companywide should always be reviewed in order to determine what are points of weakness for staff and how to further improve the training exercises.

2. **Phishing Tests**

2.1. **Test Release Schedule:** Phishing tests will be sent out companywide on intervals between 90-150 days.

2.2. **Test Results:** Failure of tests may result in additional mandatory training being provided to staff in question. Individual results will remain anonymous to the rest of staff, other than the staff involved in running the tests.

2.3. **Record Points of Failure:** It will be properly recorded who and how people are failing the tests. Again, results will remain anonymous to the greater company populace, and such information will be solely used for analysis and improvements of the tests

CLOUD SECURITY POLICY

1. Cloud Services Provider

1.1. Handler of Cloud Services: Company cloud functions will be hosted and run through Microsoft Azure Services. This helps centralize cloud functionality and security through a trusted provider. This is subject to change according to present circumstances.

1.2. Cloud Security: It will be the responsibility of those managing our Azure subscription(s) to keep updated on security services provided for our cloud products. It will be up to their discretion, with provided reasoning given, on what security services the company needs for the cloud.

1.3. Cloud Architecture: While it is the current plan for cloud functionality for company processes to be run through Azure, the company of course also provides their own cloud products. In-house cloud services may be implemented as deemed fit, provided it does not over complicate and/or break currently running services from Azure.

2. Cloud Access

2.1. Role-Based-Access: Access to cloud services will be provided based on individual role and responsibilities, only providing minimum access to meet these standards. Further access will only be provided after being given authorization by a superior and the managing party of the needed cloud service by the individual requiring access.

2.2. Appropriate Usage: Staff are expected to use their cloud access in a manner according to their role. Performing activities outside their role, using their access for personal means, and/or using their access in a harmful manner to the company can result in access being revoked, termination of employment, or appropriate law enforcement being involved should it be necessary to the action committed.

2.3. Access Privileges: Should it be deemed necessary, provided with sufficient reasoning, access to cloud services may be revoked at any time given reasonable circumstances to do so. Alternative resources should be provided in the best possible manner should the individual losing access still be expected to perform their regular duties.

NETWORK SECURITY POLICY

1. FIREWALL & NETWORK SEGMENTATION

1.1. Perimter Firewall Enforcement: Deploy next-generation firewalls (NGFW) for all internet gateways and deny any inbound traffic by default with an exception for allowed services.

1.2. **Internal Network Segmenetation:** Networks should be separated for each department and each of their purpose. For corporate users, development environments, cloud systems, and HR and Finance Systems.

1.3. **Least Privielege Network Access:** ONLY required ports, protocols, and IP should be allowed. Unused ports and services should also be disabled.

1.4. **Firewall Rule Review & Logging:** Firewalls rules should be reviewed quarterly and log allowed and denied traffic for monitoring.

1.5. **Cloud Firewall Security Groups:** Application of strict inbound and outbound filtering for cloud-hosted resources. No public access allowed to databases and/or management interfaces.

1.6. **CIS Control 13 - Network Monitoring & Defense:** To detect and respond to cyber threats by monitoring network traffic and identifying malicious behaviour.

2. INTRUSION DETECTION & PREVENTION PROLICY (IDS/IPS)

2.1. **Network-Based IDS/IPS Deployment:** Monitor inbound and outbound traffic for malicious signatures and anomalies

2.2. **Endpoint Detection Integration:** Integrate IDS/IPS with Endpoint Detection Systems (EDR) for rapid response.

2.3. **Automated Threat Response:** Automatically block suspicious IPs, domains, or attack patterns.

2.4. **Centralized Monitoring and Alerts:** Send IDS/IPS alerts to a centralized SIEM platform and define alert severity levels for prioritization.

2.5. **Regular Signature & Rule Updates:** Ensure IDS/IPS signatures are automatically updated to fight against emegerging threats

3. SECURE WIRELESS (WI-FI) NETWORK POLICY

3.1. **Enterprise Wi-Fi Encryption Standards:** Use of WPA3-Enterprise or WPA2-Enterprise for corporate wireless networks and prohibit outdated standards such as WEP, WPA

3.2. **Network Access Authentication:** Require unique user authentication for Wi-Fi access. Enforce Multi Factor Authentication (MFA) for wireless login

3.3. **Guest Network Segmentation:** A separate guest Wi-Fi should be placed for guest users to isolate and separate from internal systems

3.4. **Wireless Access Point Configuration:** For sensitive internal networks SSDI broadcasting should be disabled. Default admin credentials on all access points should be enforced.

3.5. **Wireless Monitoring & Rogue AP Detection:** Detect and block unauthorized wireless access points that are connected to the network.

4. IMPLEMENTATION OF CIS CONTROLS 12 & 13

4.1. **CIS control 12 - Network Infrastructure Management:** To secure, maintain, and continuously manage network infrastructure to reduce attack surfaces and unauthorized access.

4.2. **CIS control 13 - Network Monitoring & Defense:** For detecting and responsind to cyber threats by monitoring network traffic and identifying malicious behaviour

COMPLIANCE & DATA PROTECTION POLICY

1. SECURITY STANDARDS & GOVERNANCE COMPLIANCE POLICY

1.1. **ISO27001 Alignment:** Adopt the ISO 27001 as the primary information security management framework and implement risk management, access control, incident response, asset management, and continuous improvement processes.

1.2. **SOC 2 Compliance:** Align controls with SOC 2 principles. Security, Availability, Confidentiality, and Processing Integrity.

1.3. **Risk Management Program:** Perform risk assessments regularly for identifying threats that relates to customer data and corporate data.

1.4. **Vendor & Third-Party Oversight:** Cloud providers and third-party vendors should be assessed if they are ISO 27001 and SOC 2 compliant.

1.5. **Governance & Accountability:** Assign some responsibilities to the senior management and IT leadership to oversee compliance.

2. DATA PRIVACY & REGULATORY COMPLIANCE POLICY (GDPR & PIPEDA)

2.1. **GDPR & PIPEDA Compliance Requirements:** TechInnovate must follow GDPR and PIPEDA rules relating to consent, data handling, and breach notification, to ensure that customers understand how their data is being used and handled.

2.2. **Customer Data Rights Management:** Customers must be able to request access to their data, update and correct any inaccurate information, and ask for their data to be deleted upon their request.

2.3. **Data Collection Limitation:** Only necessary data should be collected for the reason to reduce unnecessary data leak and privacy risks.

2.4. **Breach Notification Procedures:** If a data breach happenes, TechInnovate must notify affected customers, regulators, and stakeholders within a required timeframe.

2.5. **Privacy Impact Assessments:** New system implementation and major changes must be reviewed, ensuring that they do not introduce any type of privacy risks.**sdf**

3. DATA PROTECTION & ENCRYPTION POLICY

3.1. **Database Encryption:** All customer databases must be encrypted using strong encryption standards. This will protect the data even if attackers gain access to the system. The encryption reduces the impact of the data breach.

3.2. **Data Encryption in Transit:** Data sent over networks and on the internet must be encrypted. Preventing attackers to intercept sensitive information that is being sent. This is very important for employees that work remotely. Encrypting data in transit will help in protecting against publick and home Wi-Fi risks.

3.3. **Secure Backup Protection:** Backups that contain customer must also be encrypted. They should be stored securely and only authorized can access it. This will ensure that data is being protected and safely recovered in case an accident happens or occurs. Implementing this will prevent the backup data being the weak point in security.

3.4. **Data Loss Prevention (DLP) Controls:** Applying Data Loss Prevention (DLP) to TechInnovate will help with preventing of sharing customer data to unauthorized personnels.

4. COMPLIANCE TRAINING & AWARENESS POLICY

4.1. **Mandatory Compliance Training:** Employees of TechInnovate must complete regular training on privacy laws, data protection, and secure data handling. This training will help employees to understand their responsibilities and give them knowledge of their contribution to the overall security posture of the organization. This will help in reducing mistakes that would lead to data breaches. The training is also required for ISO 27001 for SOC 2 compliance.

4.2. **Secure Data Handling Awareness:** TechInnovate employees will undergo training on handling customer data properly. Including to not share data through personal email and cloud services. A guideline will help in reducing this for accidental leaks.

4.3. **Phishing & Social Engineering Awareness:** The training will include recognizing phishing emails and how to fight against, and will also work on social engineering attacks. Employees will learn how to report suspicious messages as well.

4.4. **Policy Acknowledgement & Enforcement:** The employees must acknowledge where they will understand and adhere to compliance policies. Failure to follow will result to corrective measures and clear enforcement will help with maintaining consistent compliance.

TECHNOLOGY USAGE POLICY

1. ACCEPTABLE USE OF COMPANY TECHNOLOGY

1.1. **Work-Related Use Only:** Use of company systems will be strictly for work purposes only. Any unnecessary or personal activities and or anything that is not work related are not allowed on company devices. By implementing this, it will reduce threat exposure to malware and malicious websites.

1.2. **Prohibit Content Access:** Access to inappropriate, harmful, or illegal conten on company-issued devices is strictly prohibited. To make sure that these kinds of site are blocked will help in reduducing the surface attack of the organization.

1.3. **Responsible Internet Usage:** When using company systems, employees should use the internet responsibly. Safe browsing helps will protect systems from drive-by downloads and malicious ads.

1.4. **Monitoring & Enforcement:** TechInnovate may monitor company systems for ensuring the acceptable use. Operating systems and antivirus software must always be updated to their latest versions and patches.

2. PERSONAL DEVICE & REMOTE ACCESS POLICY

2.1. **Bring Your Own Device (BYOD) Rules:** The employees using their own personal devices must follow a certain company policy in regards to sercurity requirements. The devices should must update their operating system, software, antivirus, and screen locks as well. Devices that does not meet the requirement will not be able to access company systems. This policy will help in reducing the risk of data risk exposure.

2.2. **Mandatory VPN Usage:** Employees are required to use a company-approved VPN when accessing company systems remotely. The VPN encrypts data and will protect it from interception of public or home Wi-Fi networks.

2.3. **Secure Network Access:** Employees that work remotely should avoid the usage of public Wi-Fi without any type of protection. Whenever an employee uses a public Wi-Fi, the use of VPN is mandatory.

2.4. **Device Loss & Theft Reporting:** Lost or stolen devices must be reported by the employees immediately. This quick action will allow the IT department to lock and wipe the devices remotely. Helps in preventing unauthorized access to company data.

3. SOFTWARE INSTALLATION & APPLICATION CONTROL POLICY

3.1. **Authorized Software Only:** Downloading or installing any softwares without the approval of IT department is not allowed. Unauthorized software can cause a lot of major risks for the company. By restricting downloads, it will help with maintaining the security of the system.

3.2. **Software Whitelisting:** TechInnovate has a list of approved applications and systems that the employees are allowed to use. This reduces the risk of running malicious programs. An approval for new tools for the employees should be looked in to first before getting approved, by doing this it will keep the system environment controlled and secure.

3.3. **Patch & Update Management:** Software that are approved must be kept up to date with security patches. Softwares that are outdated should not be used anymore without it being updated first.

3.4. **Prohibition of Pirated Software:** Usage of pirated software is very strictly prohibited. Most pirated software carry the risk of having malicious file hidden under it. Usage of pirated software also creates legal risks for the company

4. SHADOW IT & DATA PROTECTION POLICY

4.1. Approved Applications for Data Storage: When storing and sharing company data, employees must only use IT-approved application. Personal cloud storage and unapproved file-sharing apps are prohibited.

4.2. Shadow IT Prevention: TechInnovate will high discourage shadow IT through policies and training. Instead of finding their own solutions, employees should request IT support.

4.3. Data Leakage Prevention Awareness: Employees will be trained on how data leakage occurs. Awareness will help reduce accidental data exposure. Employees will play a key role in protecting company data.

4.4. Monitoring & Auditing Usage: IT will monitor network traffic and application usage to fight against shadow IT. Auditing will help identifying unapproved tools early. Allowing IT to address risks before data is lost and monitoring supports overall security goals.

REGULAR SECURITY AUDITS & RISK ASSESSMENT

1. Security Audit & Compliance Review Policy

1.1. Annual Internal Security Audits: TechInnovate will conduct internal security audits quarterly. The audits will help with checking whether the employees an/or the systems are following company security policies. The internal reviews will be useful for finding gaps in access controls, data handling, and security practices.

1.2. Annual External Security Audits: External security audits will be performed by third-party assessons twice a year. External auditors can help with an unbiased view of the company's security posture and can contribute in helping what to do as their next step. These will help in identifying compliance gaps and align with standards like ISO 27001 and SOC 2.

1.3. Compliance Gap Identification: Audit results is going to be used to identify any missing controls or weak security areas. The findings will be documented and reviewed by the management.

1.4. Audit Remediation Tracking: All audit findings must be tracked until they are fixed. IT and management will assign deadlines and responsibilities

2. Vulnerability Assessment and Remediation Policy

2.1. Quarterly Vulnerability Assessments: TechInnovate will conduct vulnerability assessments every quarter across all systems. Regular scanning will help with

identify weaknesses that appear over time. Frequent assessments reduce exposure to known threats.

2.2. **Severity-Based Risk Prioritization:** Identified vulnerabilities will be categorized from low to critical severity. Critical and high-risk issues will be fixed first to reduce the most serious threats. Lower-risk issues will be scheduled based on impact.

3. Continuous Monitoring and Threat Detection Policy

3.1. **SIEM Deployment:** SIEM tools collect and analyze logs from multiple systems. This helps detect unauthorized access and abnormal behavior. Centralized monitoring improves incident visibility.

3.2. **Endpoint Detection and Response (EDR):** These tools monitor endpoints for malware and suspicious actions. EDR helps stop attacks before they spread. This is especially useful for remote and personal devices.

4. Disaster Recovery and Business Continuity Testing Policy

4.1. **Backup Testing:** Backups will be tested regularly to ensure they work properly. A backup is useless if it cannot be restored. Testing helps verify data integrity.

4.2. **RTO and RPO Validation:** Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) will be reviewed and tested. RTO defines how fast systems must be restored, and RPO defines how much data loss is acceptable