INTERNAL EMPLOYEE SECURITY POLICY

1. CIA TRIAD

Confidentiality—

- Protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data.
- A failure to maintain confidentiality means that someone who shouldn't have access has managed to get it, through intentional behavior or by accident. Such a failure of confidentiality, commonly known as a breach, typically cannot be remedied.

Integrity—

- Protect the data from being sniffed and interpreted, typically by encrypting it.
- Ensure that the transmission has not been altered (data integrity).
- Another example of a failure of integrity is when you try to connect to a website and a malicious attacker between you and the website redirects your traffic to a different website. In this case, the site you are directed to is not genuine.

Availability—

- Availability means that information is accessible by authorized users
- If an attacker is not able to compromise the first two elements of information security (see above) they may try to execute attacks like denial of service that would bring down the server, making the website unavailable to legitimate users due to lack of availability.

2. Access Control

- Programmers may only code on official machines provided by company.
- Disable USB ports and only authorized person may install and uninstall the applications.
- Random monitoring will be required.
- Prevent copying of code to an external device.
- Prevent uploading code to personal email.
- Prevent committing code to an unauthorized repository.
- Mac id restrictions
- No DB access to developers

3. Auditing security activities

- Monitoring security-relevant events to provide a log of both successful and unsuccessful (denied) access.
- Reduce cost by shutting down or repurposing extraneous hardware and software that you uncover during the audit
- Prove the organization is compliant with regulations – HIPAA, SHIELD, CCPA, GDPR, etc.
- Maintain a threat catalog of all discovered risk vectors

Audit to be performed like: -

- Insufficient password complexity
- Over permissive ACLs on folders
- Inconsistent ACLs on folders
- Non-existent or insufficient file activity auditing
- Non-existent or insufficient review of auditing data
- Correct security software and security configurations on all systems
- Only compliant software installed on systems
- Data retention policies followed
- Disaster recovery plans updated and tested
- Incident response plans updated and tested
- Sensitive data stored and protected correctly with encryption
- Change management procedures followed

4. Remote Access Policy

Employees may work remotely on a permanent or temporary basis. Permanent remote work employees should indicate their primary working address in a remote working agreement. This contract will also outline their responsibilities as remote employees.
Remote access policies validate a number of connection settings before authorizing the connection, including the following:

- Remote access permission
- Group membership
- Type of connection
- Time of day
- Authentication methods
- Advanced conditions such as access server identity, access client phone number, or Media Access Control (MAC) address
- Whether user account dial-in properties are ignored

- Whether unauthenticated access is allowed
- After the connection is authorized, remote access policies can also be used to specify connection restrictions, including the following:
- Idle timeout time
- Maximum session time
- Encryption strength
- IP packet filters
- Advanced restrictions:
- IP address for PPP connections
- Static routes

Additionally, restrictions based on the following settings:

- Group membership
- Type of connection
- Time of day
- Authentication methods
- Identity of the access server
- Access client phone number or MAC address
- Whether unauthenticated access is allowed

5. FILE STORAGE

To keep your data secure, every file should have a designated storage location that the organization can control, and employees should be trained on the risks associated with storing company documents in unsecured places.

Some policies regarding Backup for files: -

- You specify a different management class in an Include statement to change the management class for the file. The backups are managed based on the old management class until you run another backup.
- Your administrator deletes the management class from your active policy set. The default management class is used to manage the backup versions when you back up the file again.
- Your administrator assigns your client node to a different policy domain and the active policy set in that domain does not have a management class with the same name. The default management class for the new policy domain is used to manage the backup versions.

6. USER ACCESS CONTROL

Access should be given according to the roles in the company. Higher the position higher will be the access to the records of the company. All user accounts in your organization don't need the same level of access. When people have too much permission, then the data is prone to more risk.

Things to consider mainly: -

User Access Account Management

- All additions, deletions, suspensions and modifications to user accesses should be captured in an audit log showing who took the action and when.
- These procedures shall be implemented only by suitably trained and authorized Employees
- A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.
- Users will normally be limited to only one user account for each individual information system for non-administrative purposes. Any variations from this policy must be authorized by the Senior Responsible Owner (SRO) or, where applicable, the Authority.
- All user accounts that have not been accessed for an agreed period, without prior arrangement, must be automatically disabled.
- Access to systems by individual users must be authorized by their manager or where applicable, the Authority.
- All changes to privileged accounts must be logged and regularly reviewed

Monitoring User Access

- Systems will be capable of logging events that have a relevance to potential breaches of security.
- User access will be subject to management checks.

Password Management

- Passwords must not be shared with any other person for any reason.
- All default system and vendor passwords must be changed immediately following installation.
- All DWP information systems must support strong password management techniques (such as: length, complexity, aging, history, account lockout).
- All DWP information systems must technically force new user accounts to change the initial password upon first use to a strong password and thereafter on a regular basis.

7. CYBER ATTACKS (CYBERSECURITY AWARENESS)

The company should train their employees and staff about the latest and prevailing cyber-attacks that are mostly happening in the current era. Like social engineering attacks, phishing mails etc.

List of most common employee mistakes and their solutions: -

1. Opening Emails from Unknown People

Solutions:

- Advise employees not to open emails from people they don't know.
- Advise employees to never open unknown attachments or links.

2. Having Weak Login Credentials

Solutions:

- Require employees to use unique passwords
- Add numbers and symbols to a password for increased security. For example, change "Seattle" to "S3att!e."
- Create rules that require employees to create unique, complex passwords of at least 12 characters; and change them if they ever have reason to believe that they have been compromised.
- Take the headache out of this by using password manager software to automatically generate strong individual passwords for multiple apps, websites and devices.

3. Leaving Passwords on Sticky Notes

Solutions:

- If employees must write down passwords, ask that the paper copies are kept inside locked drawers.

4. Having Access to Everything

Solutions:

- Set up tiered levels of access, giving permission only to those who need it on each level.
- Limit the number of people who can change system configurations.
- Don’t provide employees with admin privileges to their devices unless they really require such set up. Even employees with the admin rights should only use them as needed, not routinely.

5. Lacking Effective Employee Training

Solutions:

- Provide annual cyber security awareness training. Topics could include:
- Reasons for and importance of cyber security training
- Phishing and online scams
- Locking computers
- Password management
- How to manage mobile devices
- Relevant examples of situations

6. Not Updating Antivirus Software

Solutions:

- Set up all system updates to take place after work hours automatically.
- Don't let any employee, no matter what their title; opt out of this company policy.

7. Using Unsecured Mobile Devices

Solutions:

- Every device should be password protected.
- If a device is lost or stolen, have a point of contact to report this to and steps taken to deactivate the device remotely.
- Use endpoint security solutions to manage mobile devices remotely.
- Don’t conduct confidential transactions using untrusted public Wi-Fi.

8. PROTECT PERSONAL AND COMPANY DEVICES

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. Advice employees to keep their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade complete antivirus software.
- Install security updates of browsers and systems monthly or as soon as updates are available.

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

9. NETWORK SECURITY

Internal Network should be protected by an enterprise-grade firewall/IDS/IPS system and utilize Network segmentation to keep the Network secure. Network should be protected against DDoS attacks, as well as other well-known Network attacks. It should scan internal Network for vulnerabilities and document remediation.

1. Network Device Security

- Patches and security updates should be applied regularly as soon as vendors release them.
- All services that are not in use should be disabled.
- Each employee should be assigned an NDA about not sharing the details of devices deployed within the perimeter.
- The company should maintain ACL to regulate UDP and TCP traffic.

2. Internet Access

- Policies relevant to internet access include all hose that automatically blocks all websites identified as inappropriate, especially those related to social media platforms.
- In an organization, the internet and network are the same things as it connects crucial assets of the organization such as account sections, server, and so on. Before wielding, access to the internet should be thoroughly monitored and filtered appropriately

3. VPN

- VPN is designed to be used exclusively on organization-owned computers as it provides a way to secure data as it travels over an untrusted network.
- Remote access of company computers from home over the internet is to be denied to avoid malicious access.
- L2TP with IPsec should be applied to provide adequate protection for those who are trying to access organizations' computers remotely. Firewalls should also be set to filter client traffic.

4. Port Communication

- Only essential services such as HTTP should be left open even when they are not in use, otherwise, all other ports, whether outbound or inbound, should be strictly blocked for unnecessary services.
- Presence of several needless ports running open increases the chances of a breach to a system.
- Therefore, ports that are linked directly to the internet should be limited to or marked as ports in inbound connection or use only authorized communication services.

5. Wireless LAN

- MAC address which changes randomly
- Closed network with multiple incorrect SSID
- Beacon frames from the unsolicited access point
- Duplicated MAC addresses on frames

6. Firewall Rules

- Every time a user connects to an insecure open network, they open access gates for potential attackers to infiltrate the system
- For dedicated server access, the identity of the server is hidden by employing a proxy firewall between the remote user and the dedicated server.
- In case of traffic filtering based on destination and source port/IP address, then a packet-filtering firewall should be placed as it also increases the speed of transmission as well.
- However, when transmission speed is not of importance, then the configuration of state table inspection may be appropriate as it validates the connection dynamically and as well forwards the packet.
- Where there is a need to provide extra security measures for an organization's internal network, NAT should be used as a complement to the firewall.

- Finally, you can employ IP packet filtering if there is a need for a higher level of regulation other than preventing communication between an IP address and your server.

7. Network Intrusion

- For the extreme line of defense, IDs should be housed for anomaly monitoring and detection of unauthorized access as antivirus and firewall measures are not sufficient.
- To mitigate elevated privileges, altered permission, inappropriate auditing rights, inactive users, change of registry and much more, use Advance Antivirus with inbuilt IPS/IDS.
- IDS software's are configured over OS while intercepting IDS for software's are deployed as hardware application fundamentally due to performance reasons.

8. Proxy server

- Proxy servers are used for both defensive and offensive purposes and typically reside between a user and a server.
- All services should have a logging facility
- A proxy should not accept outside connections
- The proxy should run on the most up-to-date software and patches.

9. Secure Communication

- Data conveyed in an unencrypted form through various channels such as routers and switches on the network is susceptible to attacks such as SYN flooding, session hijacking, spoofing and sniffing.
- Ensure that MITM attacks will not tamper data being conveyed.
- Make sure that any unauthorized individual between the source and the server will not breach the conveyance channel.
- The identity of computers and people who will send packets must be authenticated.

10. Demilitarized zone

- Servers or systems such as emails, databases, web servers, and so on, that require access to the public internet, must be deployed on a specific subnet that separates outside from inside. This is to avoid the possibility of attacks by black hats, as public domains are easy to access.
- The primary goal of network security is to ensure the confidentiality, availability, and integrity of every asset within the network's perimeter.

10. ADDITIONAL MEASURES

To reduce the likelihood of security breaches, instruct the employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible.
- Change all account passwords at once when a device is stolen.
- Report security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action.