MAXX ENERGY

SECURITY POLICY TABLE OF CONTENTS

AUGUST 21, 2024

SECURITY IS EVERYONE'S RESPONSIBILITY

Watch Security Video

Maxx Energy Security Team

MAXX ENERGY

ACCEPTABLE USE POLICY

AUGUST 27, 2024

Watch AUP video

Purpose & Scope

The purpose of the Acceptable Use Policy (AUP) is to provide a set of guidelines and rules that outline how employees, contractors, and other users can access and use an organization’s information systems, networks, and data. The purpose of the policy is to protect the organization’s assets and ensure that users understand their responsibilities in maintaining the security and integrity of the organization's resources.

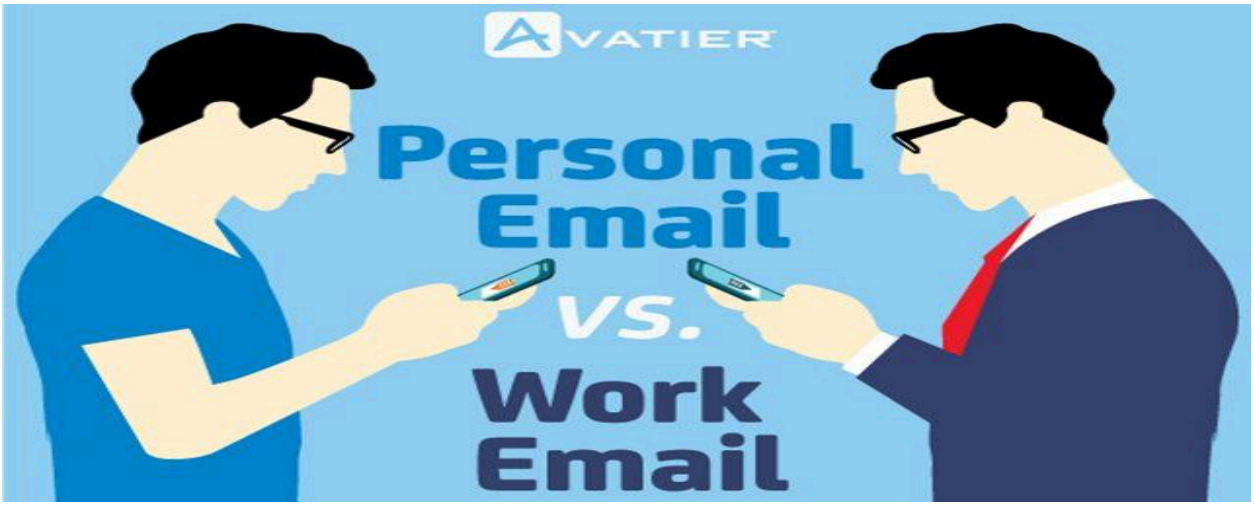
1. It is everyone's responsibility to use company equipment and electronic systems in a responsible way. All reasonable steps are to be taken to preserve any hardware you are given to use and also to protect any data you have access to that originates from and or belongs to the company. Employees must use the organization's resources responsibly and for legitimate business purposes. This includes following all applicable laws, regulations, and company policies.

2. You are prohibited from using any social media, shopping, gaming or any other website for personal reasons. For additional protection, Maxx Energy employs web servers that only have specific websites green listed to allow access from our ip addresses. Any other website will be automatically denied access to our network. If any exceptions are needed requests are to be formally requested and documented in writing. Users are expected to use the organization's

resources primarily for work-related activities that support the organization's mission and goals.

- Users should not engage in activities that consume excessive bandwidth or resources, such as streaming non-work-related videos, gaming, or downloading large files unrelated to work.

3. Users are responsible for safeguarding their accounts, passwords, and access credentials. They must not share passwords or allow unauthorized individuals to access the organization's systems.



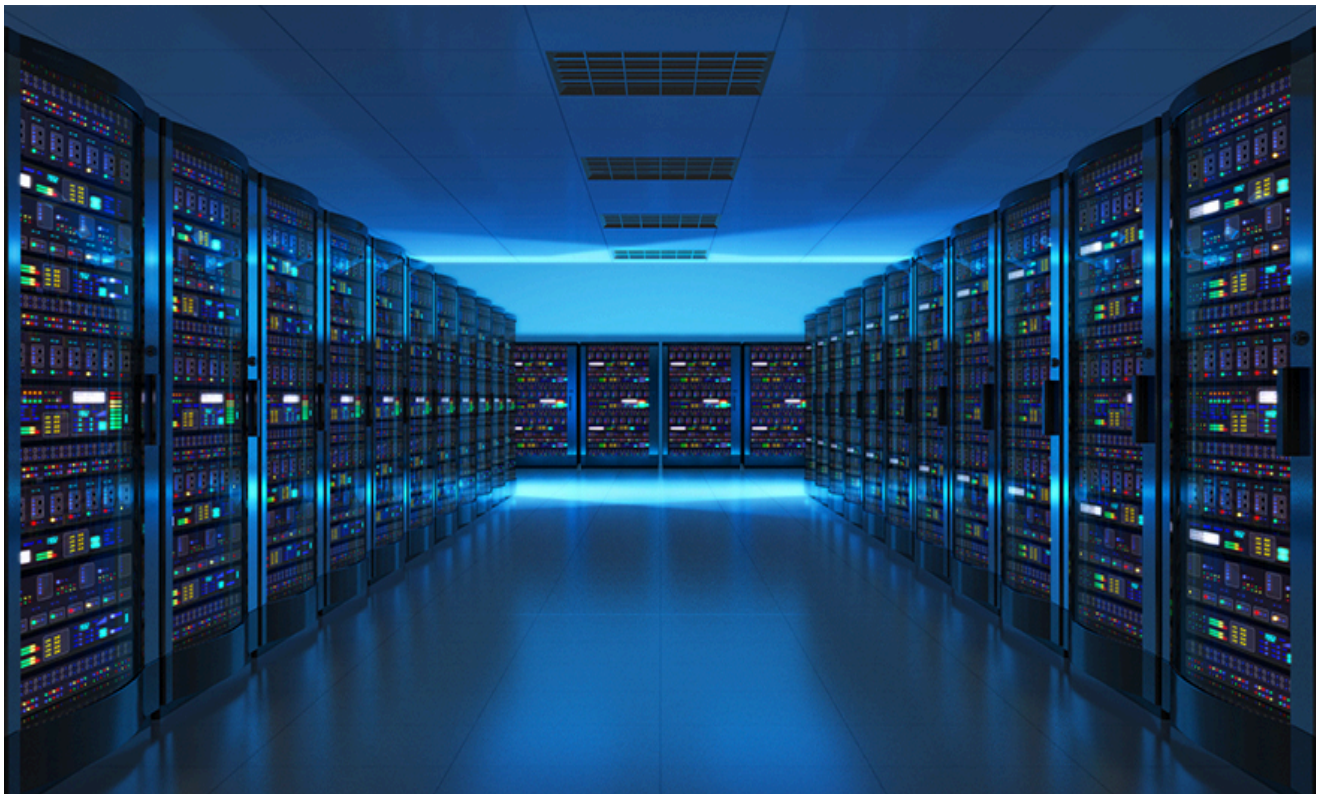
4. No personal emails are to be sent from your business account. All corporate email accounts, while not actively under surveillance, will be permanently saved and owned totally by Maxx Energy.
5. All company equipment with a storage device to be operated in an encrypted state. Users must protect the confidentiality of the organization's sensitive information, including customer data, intellectual property, and trade secrets.
6. If you are issued a company Mobile Phone any office applications on the phone may be wiped at any time. All company phones will have a “find my device” application installed to wherein the general location of your phone can be tracked at any time. If at any time your phone is lost it is to be immediately reported to the security department.
7. Users must not engage in any illegal activities using the organization's resources, including but not limited to hacking, fraud, copyright infringement, and unauthorized access to systems.

8. The use of organizational resources to create, store, or distribute content that is discriminatory, harassing, or otherwise offensive is strictly prohibited.
9. Users must not attempt to bypass or disable security controls, such as firewalls, antivirus software, or access restrictions.
10. Users are responsible for reporting any known or suspected violations of the AUP to the appropriate authority, such as the IT department or a designated compliance officer.
11. Violations of the AUP may result in disciplinary action, up to and including termination of employment or contract. The policy should outline potential consequences, which may vary based on the severity of the violation.
    - **Protection Against Retaliation**: Users who report violations in good faith will be protected from retaliation.
12. In cases of illegal activity or serious misconduct, the organization may pursue legal action against the violator.
13. The AUP should be reviewed regularly (e.g., annually) to ensure it remains relevant and effective in addressing new technologies, risks, and organizational changes.
14. All users must acknowledge that they have read, understood, and agree to comply with the AUP. This acknowledgment can be collected through a signed document or an electronic agreement.

Regular training and communications are important to ensure that the policy is understood and followed by all users.

NETWORK SECURITY POLICY

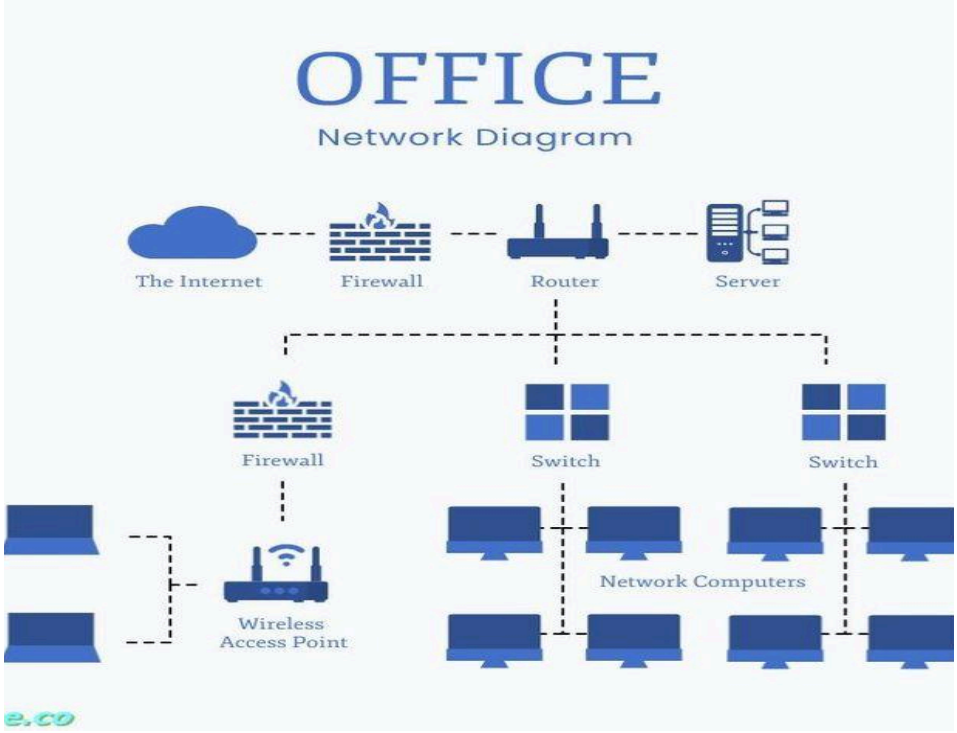
Updated 08-27-2024



Watch RBAC video

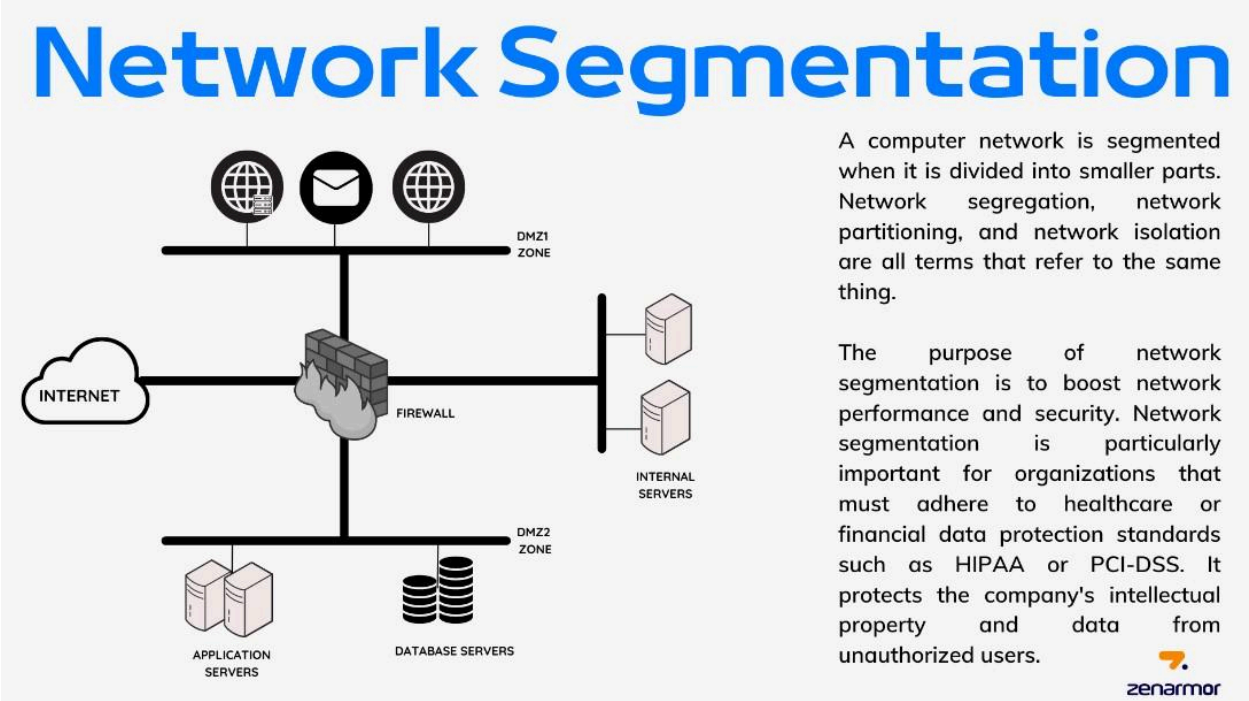
The Network Is The Electronic Backbone Of the Company

by **Security Team**



Network closet access shall only be approved and documented by network administrators!

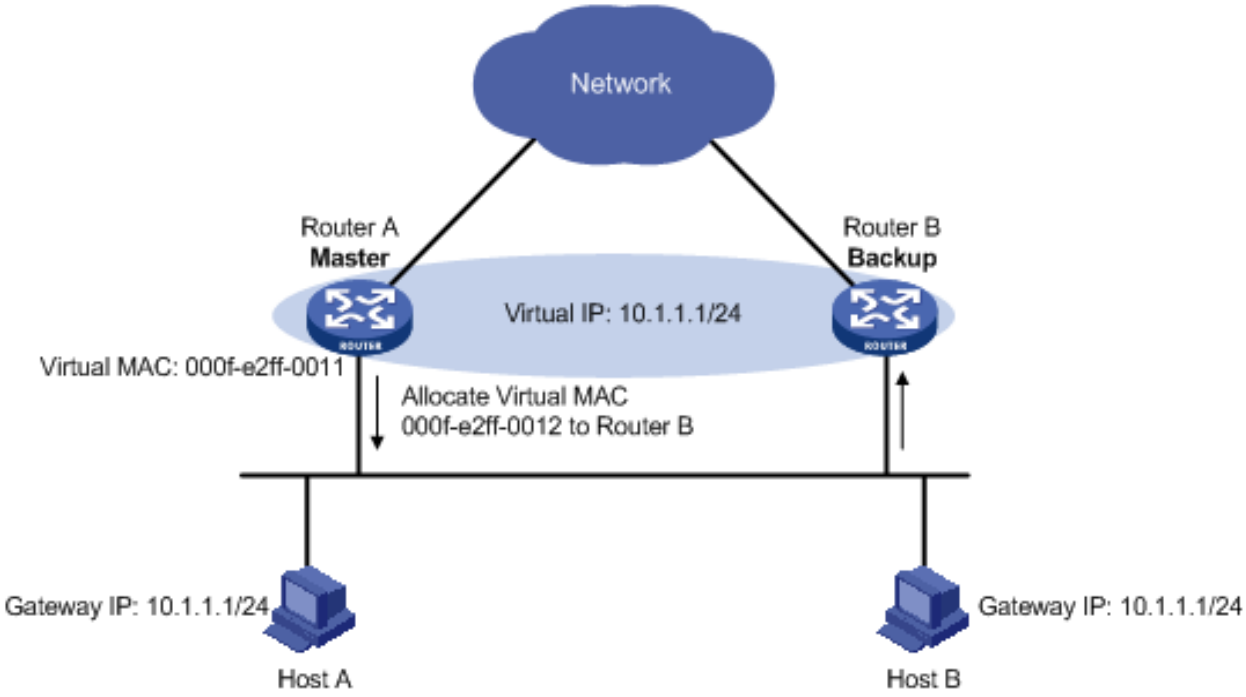
1. Only network admin employees will have access to the network closet.



2. Network admins may not access Management, Sales, Accounting, Human Resources or any other operational department databases nor will any other department have access to Network Administration. They may only access hardware and software systems to the extent that network connections are supported for reliability, redundancy and speed.

3. Network closets will be secured with electronic door locks using company provided card tokens to be swiped and documented with time and employee numbers.

4. Before an admin can access the network, multi factor authentication must be used in order to log into company systems.



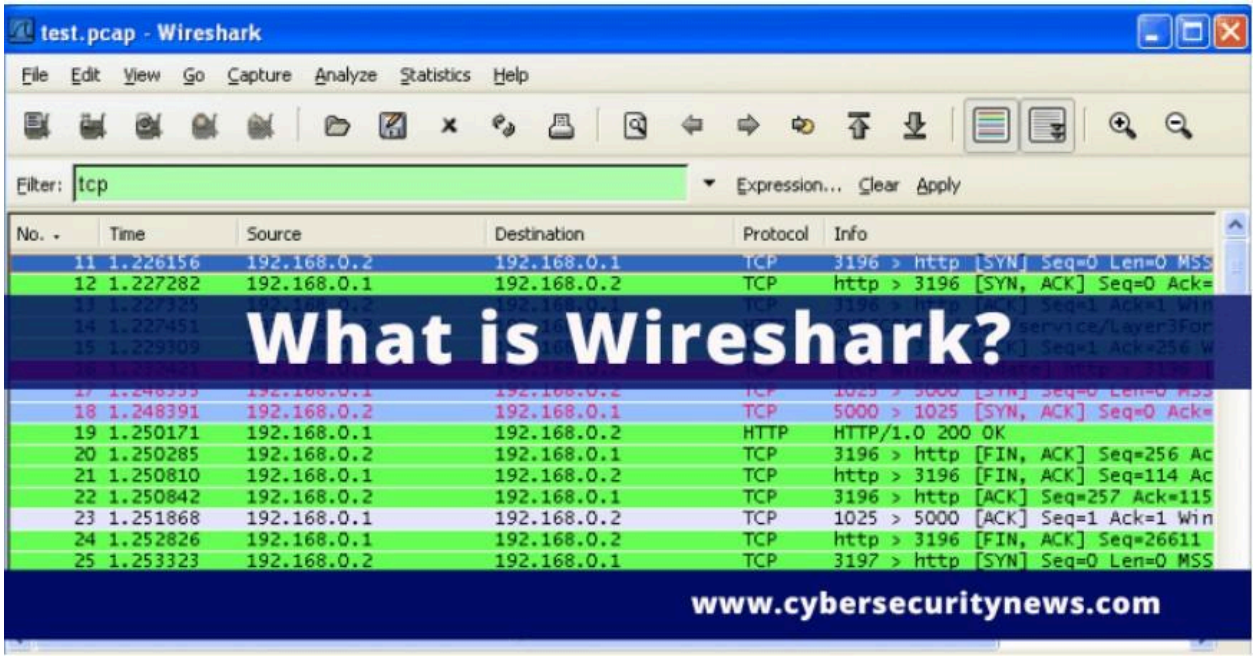
5. Each office is to have two routers utilizing the same NIC id for redundancy and efficiency.

Basic Subnetting

Subnet	Network Address	Host Range	Broadcast Address
0	192.168.1.0 /27	192.168.1.1 to 192.168.1.30	192.168.1.31
1	192.168.1.32 /27	192.168.1.33 to 192.168.1.62	192.168.1.63
2	192.168.1.64 /27	192.168.1.65 to 192.168.1.94	192.168.1.95
3	192.168.1.96 /27	192.168.1.97 to 192.168.1.126	192.168.1.127
4	192.168.1.128 /27	192.168.1.129 to 192.168.1.158	192.168.1.159
5	192.168.1.160 /27	192.168.1.161 to 192.168.1.190	192.168.1.191
6	192.168.1.192 /27	192.168.1.193 to 192.168.1.222	192.168.1.223
7	192.168.1.224 /27	192.168.1.225 to 192.168.1.254	192.168.1.255

6. Each Department is to have its own subnetwork protected by a firewall and separated by a demilitarized zone for extra security.

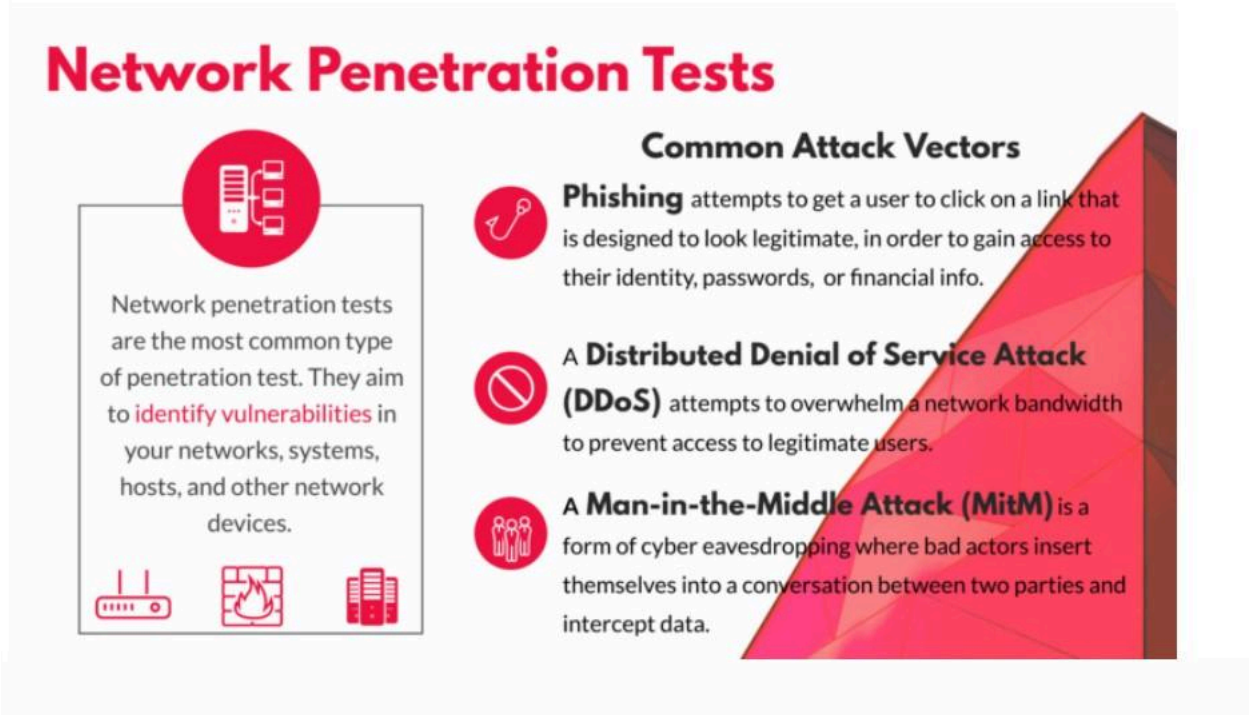
7. All Network admin to maintain current accredited Network+ Certifications.



8. Network admin will continuously monitor network during operation buy using network monitoring tools and appliances as well as manually observing packets and ram usage. In addition daily network usage log statistics will be documented and stored.

9. Temp and humidity of the network closet to be maintained in ranges of 68-71 degrees and 45-50% respectively to maintain optimal longevity and reliability of network equipment.

10. When the company budget allows, fiber optic cables are preferred to be used over ethernet cables and network admin staff are to prepare cost proposals whenever network cables are needed to be installed or replaced.



11. The security department will conduct annual red hat penetration tests to test the vulnerability of the network.

12. The Network Department shall utilize a network as a service, NAS, 3rd party provider to provide elastic network bandwidth resources as needed for unusual high demand times or outages as extra redundancy.

13. Violating the network admin policy can result in a documented written warning or firing depending on the severity of the violation at the discretion of the Human resources department.

14. Network operating policies to be reviewed, audited & updated with pertinent generally accepted standards on a bi annual basis.

15. All wifi access points are to use the most updated methods of encryption .

16. All wifi access points are to remain inside of the building. No signal shall be strong enough or pointed in such a way that signals will be reachable outside of the physical building to include parking lots and break areas.

Implementing these rules will help establish a secure network environment that maximizes and protects our organization's network while minimizing risks.

MAXX ENERGY

DATA MANAGEMENT POLICY

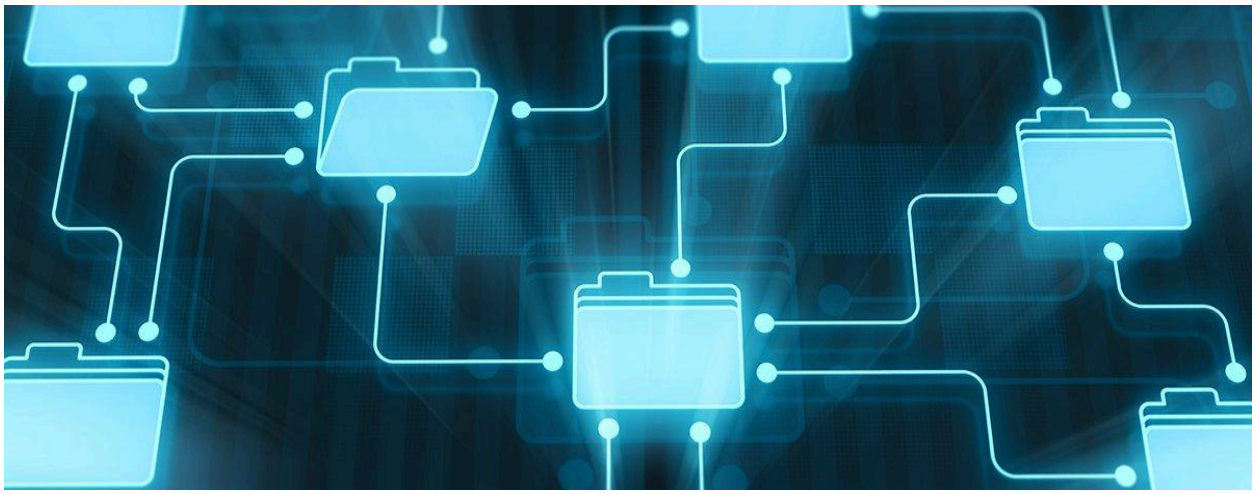
by **Security Team**

August 27, 2028

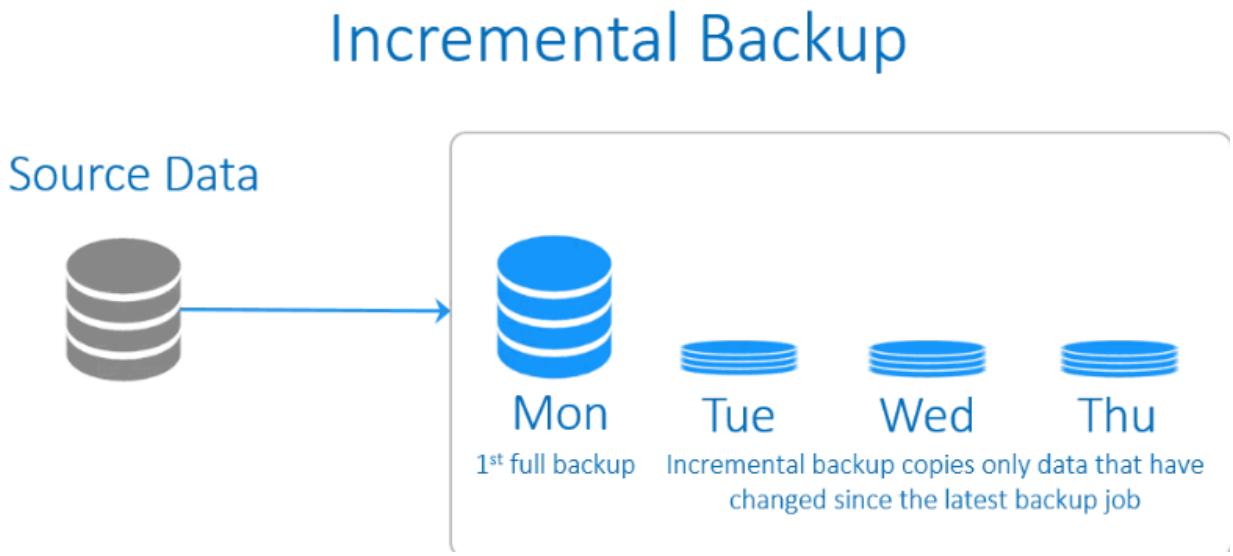
Watch Data Loss Video

⬆️DATA LOSS PREVENTION⬆️

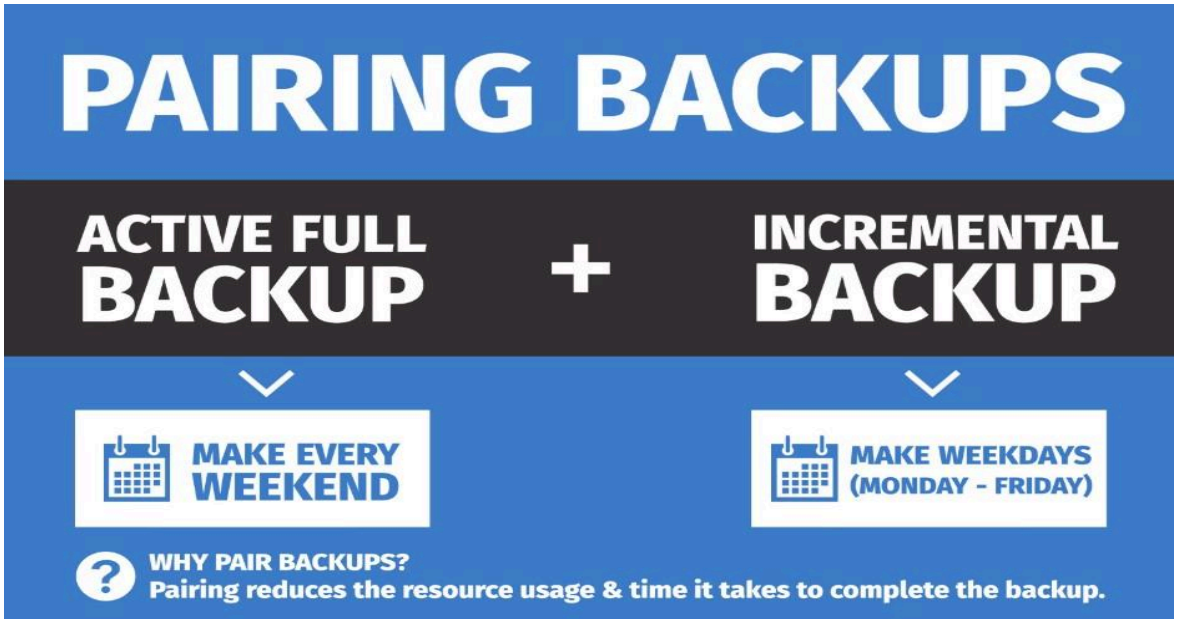
The overarching goal of our Data Management policy is to protect sensitive data, ensure compliance with regulations, reduce the risk of data breaches & provide fast uncorrupted data to all sections of the company upon request.



1. Data is to be classified, saved & segmented into three distinct files; Internal, public & confidential.
2. Confidential Data is to only and always be read, written ,shared and stored in an encrypted state at all times.
3. Complete copies of data to be stored in 2 separate locations and in 2 separate forms preferably an onsite hard drive storage system segmented off of the production network and the other off site in a cloud storage solution.



4. Incremental backups to be performed on a daily basis after production hours.



5. Full system backups to be performed on a weekly basis.
6. Company data files to be saved for no less than a two year period.
7. Decommissioned internal and public storage devices to be wiped before disposal while confidential storage devices to be degaussed and shredded.

8. Before admin can access storage protocols multi factor authentication must be used in order to log into company systems.

9. Any files shared with 3rd parties are to be approved by department heads and documented

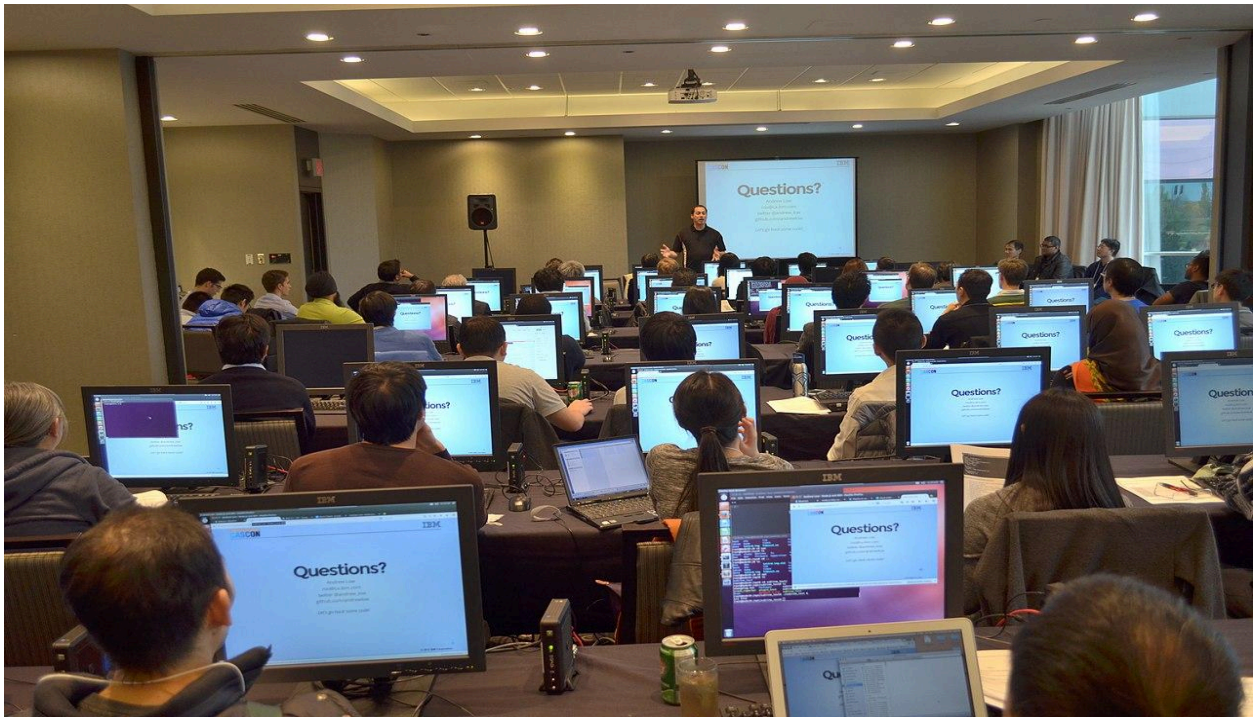
10. Data Breaches to be immediately reported upon discovery to mitigate any potential damage or repercussions.

11. Shoulder surfing is not allowed. It is forbidden to gaze upon anyone's computer screen in a solitary setting without their knowledge and acceptance. In addition, you may not make copies whether electronically or via pen and paper nor plagiarize any of your team members work.

12. Data loss prevention software to be employed and monitored

13. The original creator of a company file is responsible for conveying reading, writing and execution rights for its contents.
14. No company hardware is to leave the facility at any time.

15. The security team has the right to wipe all data associated with the companies applications from your personal mobile devices at any time.



16. Onboarding team members to be trained on methods of data security, consequences of lack of security and they are to be tested and retrained as necessary on an annual basis. (Refer to security awareness & training section for more information)
17. Failure to adhere to these rules and protocols can result in disciplinary actions.

MAXX ENERGY

PHYSICAL ACCESS CONTROL POLICY

AUGUST 27, 2024

by **Security Team**

Access Control Policy Purpose

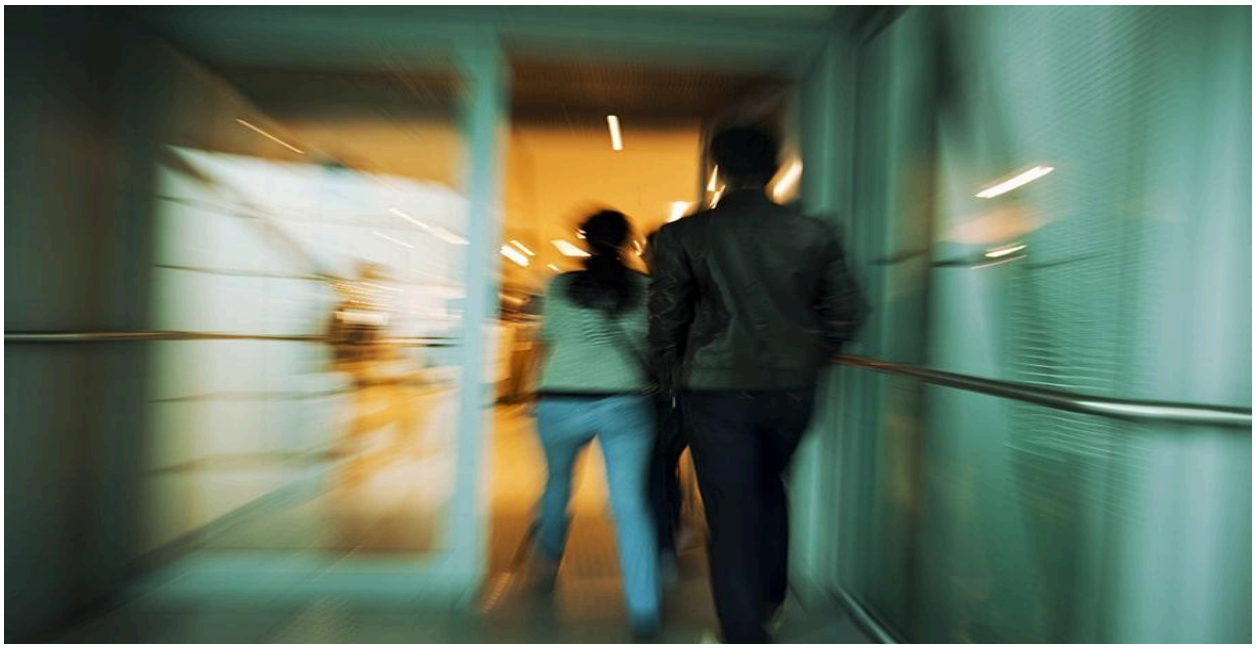
The purpose of the access control policy is to ensure that access to physical assets, information systems and data is managed securely

Watch access control video

- Team members will not park vehicles in front of nor block pathways to and through building bollards.

1. Team members are to have company identification badges on their person at all times. If you have misplaced your badge you are to obtain a temporary pass from the security office before you come into the facility and before you operate any company machines.

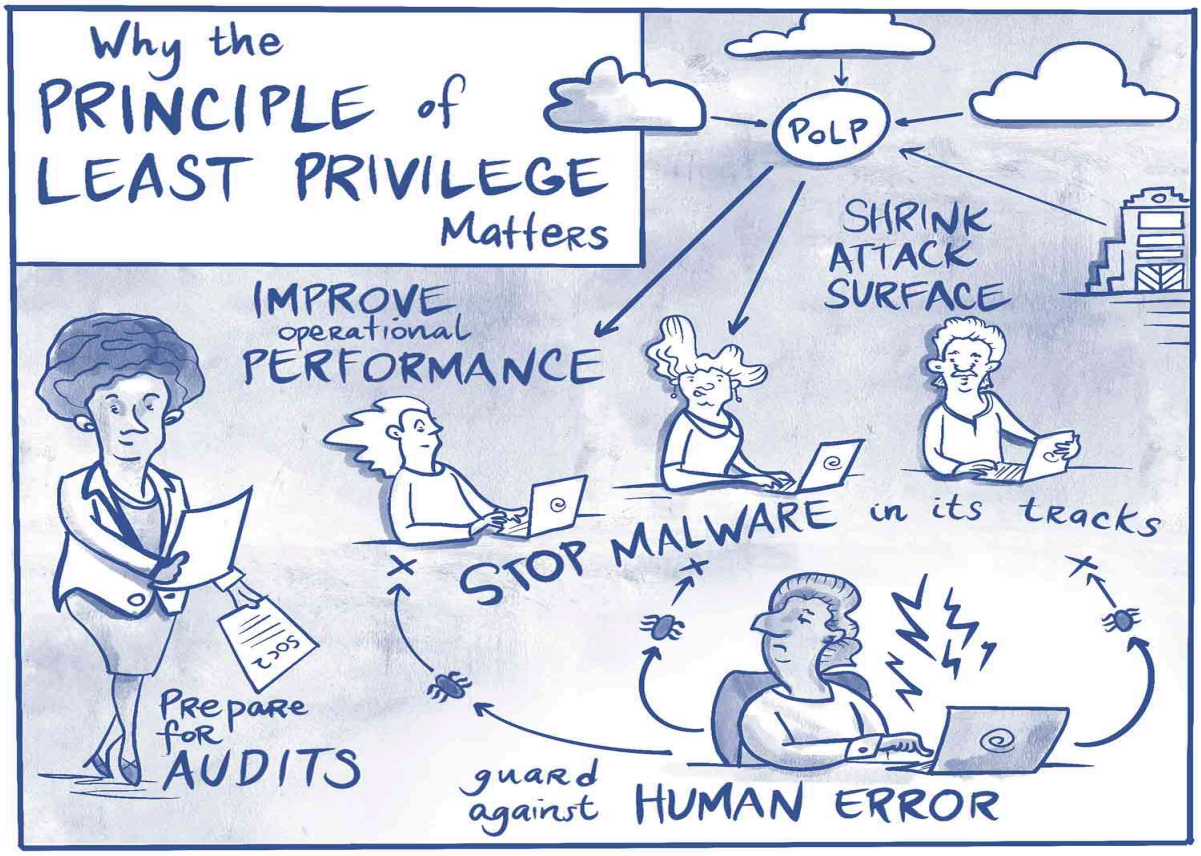
2. All passwords to operate company nodes are to be stored electronically using a password manager on your company provided browser. No passwords are to be physically written on any document. (please refer to password management policy for further information)



3. Piggy backing is not allowed. You may not hold any building access doors, any internal locked doors, or any vehicle access gates open for another team member. Your individual credentials may only be used for your individual access. There will be harsh penalties if you allow anyone access to any restricted area with your credentials.

4. All guests of team members are to be checked in at the security station and given a pass before any access is allowed inside of the building unless express consent is granted by your team leader / manager.

5. All 3rd party vendors must have appointments to perform any work inside of the building. They must establish appointments with the security team before entrance and must receive temporary badges before allowed access to any building offices or machines. In case of emergencies you may be escorted to certain areas or allowed access to specific machines only under the supervision and documentation of a security team member along with the express consent of that particular department head. (Please review Vendor Management Policy for further information)



6. Access to Company systems shall be granted on a least privilege basis. You will only have access enough to perform your specific required tasks and shall not have access or permissions to devices, storage, networks etc that are not within the scope of your job requirements.
7. All Card swipes for access to any machine or any office will be electronically recorded.

8. Video monitors will maintain 24 hr surveillance at all building entrances and exits as well as to the network room and heat air and air filter mechanicals room.
9. Remote Access to company files shall require encryption tunnels for server approval.

10. Company training to be required on a biannual basis on current access policies.
11. Access control policies will be audited and iterated as necessary on an annual basis.

Maxx Energy Security Team

PASSWORD MANAGEMENT POLICY

The password management policy is designed to help protect sensitive information by establishing guidelines for creating, storing, and managing passwords. Here are the company policies for password management.

August 22, 2024

1. Password Creation Guidelines:

- **Complexity Requirements**:Passwords must include a mix of three of the four following categories: uppercase and lowercase letters, numbers, and special characters (e.g., @, #, $).
- **Minimum Length**: Passwords must be at least 14 characters long since the longer the password, the greater the security it gives.
- Passwords must be stored in a encrypted password manager using the companies provided browser
- No passwords are to be stored in an unencrypted word file or legibly written on any physical objects.

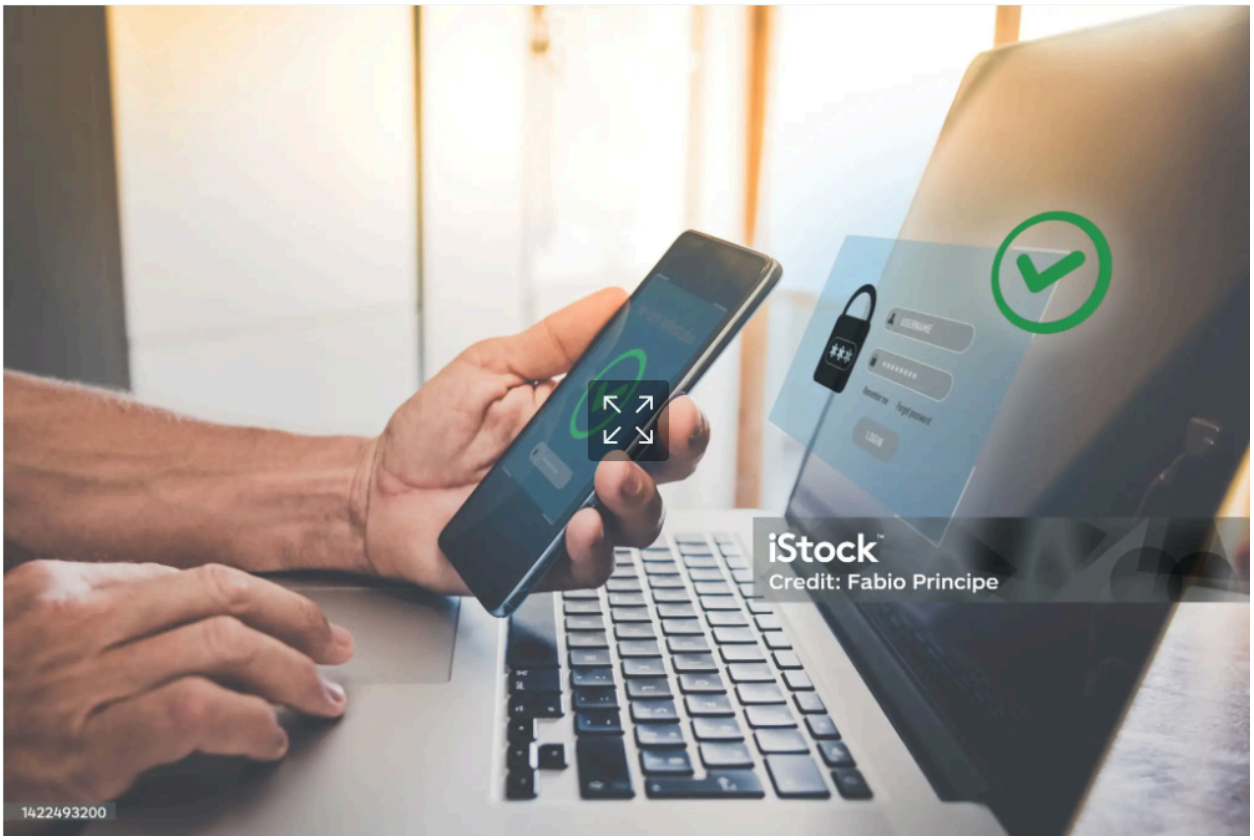
- **Prohibited Elements**: Employees must avoid using easily guessable information such as birthdays, names, or common words. Passwords mustn’t include four sequential numbers or repeated characters.

2. Password Expiration and Renewal:

- **Expiration Period**: Passwords must be changed regularly, on an annual basis.

- **Prohibited Reuse**: Employees mustn’t reuse their previous 8 passwords.

3. Multi-Factor Authentication (MFA):



- **Mandatory MFA**: Multi-factor authentication must be enabled wherever possible, especially for accessing sensitive systems. This

adds an extra layer of security by requiring a second form of verification in the form of text message codes.!!!

4. Password Storage and Management:

- **Use of Password Managers**: Employees are required to use a trusted password manager such as {x} to generate, store, and manage passwords securely. New password managers must be approved by the organization's IT department.
- **Avoidance of Written Passwords**: Passwords must not be written down or stored in plain text. If they must be written, they must be stored in a secure location.

- **Encryption of Passwords**: Any stored passwords must be encrypted to protect them from unauthorized access.

5. Account Lockout Policy:

- **Failed Login Attempts**: After 4 failed login attempts the account will lock with a lockout period of initially 15 minutes. Each additional failed

attempt increases the time until either a successful attempt or until an administrator can unlock the account.

6. Password Sharing and Transmission:

- **No Sharing of Passwords**: Passwords must never be shared with others, even within the organization. If access must be granted it must be done through official channels, such as account delegation or role-based access.
- **Secure Transmission**: If a password must be transmitted, it must be done securely, using encryption or secure communication channels. Passwords must never be sent via email or messaging apps in plain text.

7. Incident Reporting and Response:

- **Reporting Compromised Passwords**: Users must report any suspected compromise of their passwords immediately to the IT or security team. If you suspect that your account has been compromised then the security team shall likely lock your account to

contain any potential threat. This shall be explained in more detail in chapter 9 which contains the incident response policy.

- **Regular Audits**: Regular audits shall be conducted to ensure compliance with the password management policy and to detect any weak or compromised passwords.

8. Training and Awareness:

- **Employee Training**: Regular training sessions will be conducted to educate employees on best practices for password management, the importance of strong passwords, and the risks of poor password habits.(See Chapter 10 for training information)
- **Security Reminders**: Periodic reminders and tips shall be provided to reinforce the importance of following the password management policy.

9. Compliance and Enforcement:

- **Monitoring and Enforcement**: Compliance with the password management policy will be monitored, and any violations shall be addressed promptly. This may include disciplinary action up to termination depending on the severity of the violation.
- **Review and Update**: The password management policy will be reviewed regularly and updated as needed to address new security threats and changes in technology.

REMOTE ACCESS POLICY

1. Users are not allowed to sign onto remote servers without prior clearance
2. Users computer must have up to date firewall and virus protection software, company is responsible for payment for those services
3. Users are not allowed to access work servers outside of office hours.
4. Users must only connect to servers via hardwired ethernet cables over an encrypted connection.

5. Users may not connect remotely to servers using wifi connections
6. Passwords must be changed every 6 months
    - See chapter 5 password policy for further information.
7. Users cannot download files from the server unless they have been cleared by the security team, no sharing them with people who are not employed with us

VENDOR MANAGEMENT POLICY

1. Vendors have to have security policies, such as incident response, disaster recovery, and business continuity plans

2. Vendors must align with parent company's security plans
3. Vendors must conduct background checks and share them with the parent company.
4. Vendors must go through an audit every year to make sure if they're up to company standards.
5. Vendors must put all workers through the same privacy and security training for its personnel.

6. If it is found that a vendor is the reason for a security breach, they take full responsibility for a chunk of the cost of fixing it.

REMOVABLE MEDIA POLICY

1. Employees aren't allowed to bring items, such as phones, USBs, External memory drives, what have you past the turnstiles/Doors.

2. Lockers are available for you but you have to have your own lock
3. If you are found with external media capabilities past the gate, you are immediately terminated and your items are forfeit.
4. If an employee has to take out files/items, they have to have paperwork prepared and logged before it can be taken off site.
5. When the external drive/USB is turned back in, user must check it back in with the security team

INCIDENT RESPONSE POLICY

1. Insubordination will not be tolerated and failure to comply will lead to disciplinary matters up to termination.
2. Team members are to immediately report data loss incidents to their department leads and the security team.
3. **Bad Weather:** In the event of bad weather that causes electricity and wi-fi shortage or being snowed in, such as hurricanes, blizzards, earthquakes etc, It is totally fine to call off work so long as you let the

company know that you will be absent.

4. **Fire/Flood:** In the event of Structure fires or floods one should evacuate the building immediately and call the appropriate emergency service for the event in question.
5. **Injured Employee:** In the event that either you or a fellow employee gets injured you must call either for a first aid kit or dial 911

depending on the severity of the injury.

6. **Trespasser/s:** If you see an unauthorized person/people in places marked as private in any way you should call for security and, if

possible within reason, try to get a picture of the trespasser/s.

7. **Peripheral device such as USB chip:** If you find a random Peripheral device such as a USB chip make sure to give it to the security team so they can analyze it to make sure it does contain a virus or some

similar threat.

8. Compromised Device: If you even SUSPECT that your phone, laptop etc. has been hacked alert the head of security so that they can investigate. This will often mean that your account will be locked so

as to isolate the damage if the threat is real.

9. Malware Removal Process - identify and research malware symptoms- quarantine the infected systems - disable systems - remediate the infected systems- schedule scans and run databases- enable system restore and create a restore point - educate the end user.

10. Annual Updates: Annual updates will be made to this policy to address any threats and vulnerabilities that were exposed. As a result employees are expected to keep up with any new rules that come as part of the updates.
11. Bi-anual Training: Every other year there shall be training regarding all the various updates on this policy. For more details see chapter 10

Maxx Energy Security Team

SECURITY AND AWARENESS TRAINING

August 22nd, 2024

The Security awareness and training policy, as the name implies, is meant to make employees aware of the various security and training mandates.

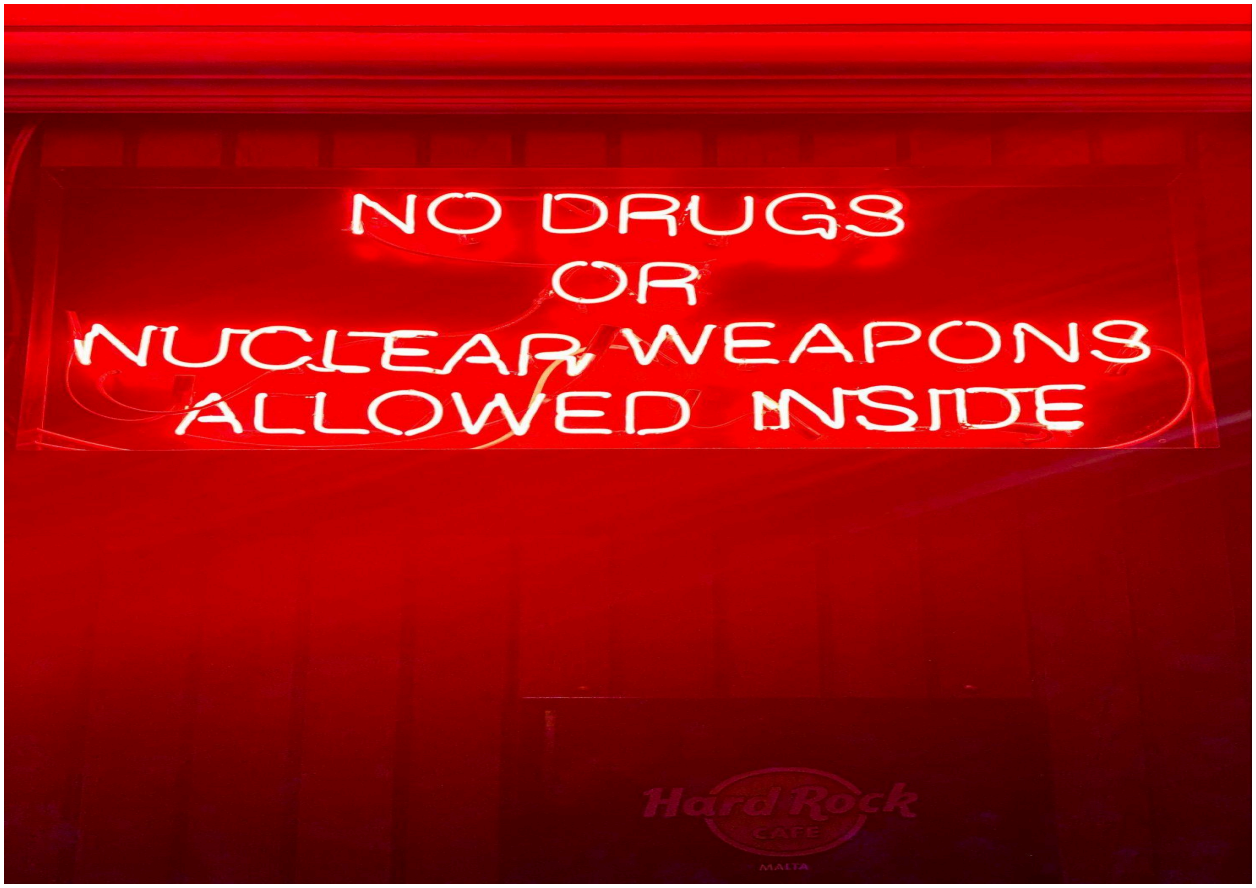
1.Mandatory training: All employees are required to participate in security awareness training.

2.Security team will periodically make email phishing attempts on team members.

3.Security team will periodically make social engineering attempts on team members.

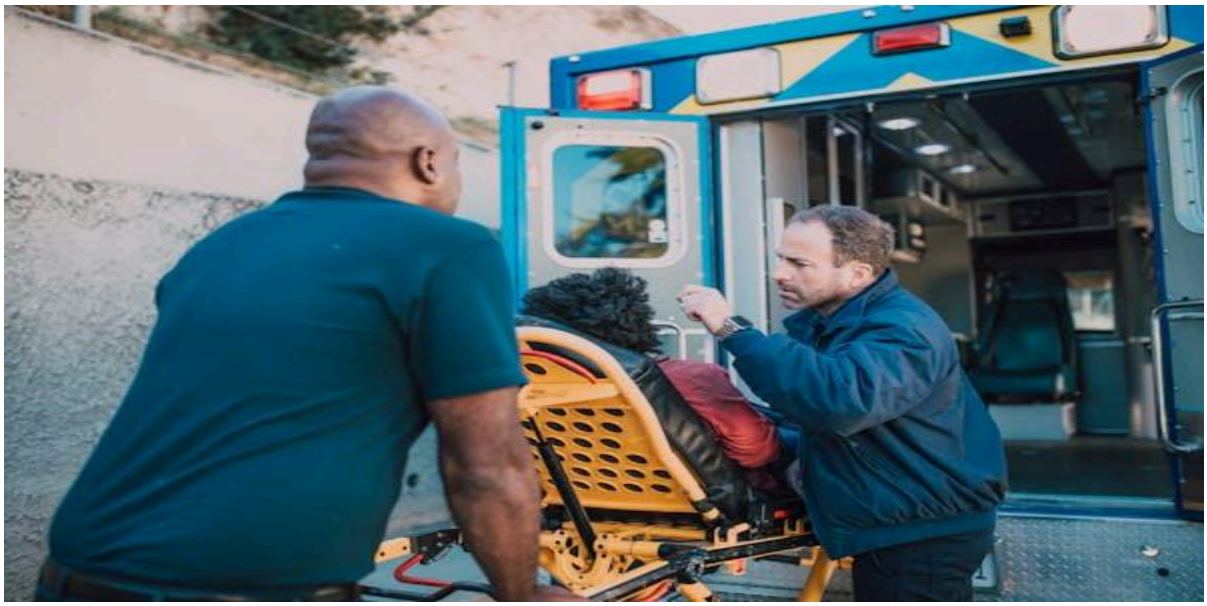
4.No weapons are allowed on company grounds at any time.

5.No non-prescribed drugs on company grounds at any time.



6.In addition to when first hired there are bi-annual company training sessions to refresh all employees' memories.

7. When an incident occurs verbally report to your team leader and to the security team. Also send them an email for documentation.



8. All department heads are to have round table meetings with their team/s once a month for security review.

CITATIONS

1. Security Video pg 2. Youtube titled “5 software tools you can't live without strong IT security Policies #Cybersecurity #antivirus” by @pcfix411RetroZone.
2. Acceptable Use Policy Video pg 3. Youtube titled “Acceptable Use Policy Explained” by DCP Technology.
3. RBAC video pg 9. Youtube titled “ What is Role-Based Access Control (RBAC)?” By delinea.
4. Data Loss Prevention Video pg 22. Youtube titled “ Data Loss Prevention #DLP Explained #Shorts” by Cyber_Short_information.

PERTINENT DEFINITIONS

Role Based Access Control- is a method that controls what users can do within a company's IT system by assigning roles and permissions to each user.

Active Directory - A database and set of services that connects users & hardware to the Network

Department Network Segmentation - A security technique that divides a network into smaller, isolated sections called subnets or segments.

Access Control Systems - Access Control Systems are electronic systems that allow authorized personnel to enter controlled, restricted or secure spaces by presenting an access credential to a credential reader

Principle Of Least Privilege - Users should only have access to the minimum level of permissions needed to perform their job functions.

Created By The Security Team

Security is Everyone's Responsibility