Clean Desk Policy

1. Overview

Sensitive documents and materials are liable to intentional or unintentional disclosure to unauthorised parties when they become unaccounted for. A Clean Desk Policy is a useful tool for helping ensure that sensitive and confidential material does not go unaccounted for or become exposed. A Clean Desk Policy in its most basic form requires employees to completely clear their desks at the end of their workday, moving items to drawers and disposing of documents that are no longer needed. This protects Company data from unauthorised access as it reduces the number of sensitive data that is available to an unauthorised person who may gain access to the Company's premises.

2. Purpose

The purpose of this policy is to establish a clear procedure and minimum requirement for maintaining a Clean Desk. It details why a Clean Desk is important for data security, as well as the methods in which this is best achieved.

3. Scope

This policy applies to all employees, contractors, temporary workers and any other personnel that may work on behalf of the company or within the company's premises.

4. Policy

4.1. All sensitive, confidential or personal information in paper or electronic form must be secured at the end of the work day, or at any time when they are not in active use.
4.2. Keys to file cabinets or other secure storage spaces must not be left on desks or in other insecure areas.
4.3. Computers must be locked at any time when they are not in active use.
4.4. Computers must be shut down at the end of the work day.
4.5. Laptops must be locked in secure drawers or secured with a locking cable.
4.6. Printed material must be removed from the printer tray without undue delay and not be left around the printing area.
4.7. When no longer needed, documents containing confidential, sensitive or personal information must be shredded or inserted into confidential disposal bins.
4.8. Whiteboards must be erased after meetings or when no longer in use.

5. Compliance

5.1. Compliance Measurement

The Infosec team will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. Exceptions

Any exceptions to this policy must be approved by the Infosec team in advance and have a written record.

5.3. Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Email Policy

1. Overview

Email has become the primary method of business communications, both within and between organisations. It is essential that email is used appropriately and securely so that it cannot compromise the security or integrity of the Company's data, systems or operations.

2. Purpose

The purpose of this policy is to promote the secure and appropriate use of email within the Company.

3. Scope

This policy applies to all employees, contractors, temporary workers and other personnel using email addresses or systems owned by the Company or operated on behalf of the Company.

4. Policy

4.1. All use of email must be compliant with the Company's policies on ethical conduct and security of business data.

4.2. All use of email must be in line with proper business practices and relevant to job duties.

4.3. The Company's email addresses or systems shall not be used for creating, distributing or accessing any offensive or illegal material, including but not limited to material with offensive comments about gender, race, age, sexual orientation or religious beliefs.

4.4. Any offensive material received in email must be reported to the IT Department and Human Resources without undue delay.

4.5. Usage of Company-owned email addresses and systems for personal use should be limited to minimal and incidental use.

4.6. Commercial and business related uses not part of the Company's business using Company-owned email addresses or systems is prohibited.

4.7. Email received to Company email addresses may not be automatically forwarded to email addresses not owned or operated by the Company.

4.8. Individual email addresses forwarded to email addresses not owned or operated by the Company must not contain any sensitive or confidential information.

4.9. The creation or forwarding of chain or joke letters from Company email addresses or systems is prohibited.

4.10. The Company may monitor and record any and all email messages received or sent by email addresses or systems owned or operated by the Company.

4.11. The Company does not necessarily monitor all email activity, but retains the right to do so.

5. Compliance

5.1. **Compliance Measurement**

The Infosec team will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. **Exceptions**

Any exceptions to this policy must be approved by the Infosec team in advance and have a written record.

5.3. **Non-Compliance**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Internet-Use Policy

1. Overview

While the internet has become essential for many business operations, it also comes with risks. It is essential that the internet is accessed in a secure manner to prevent exposure of company data or the company network, and is not misused to conduct non-business related purposes.

2. Purpose

The purpose of this policy is to protect Company devices and the Company network from inappropriate and harmful use.

3. Scope

This policy applies to all employees, contractors, temporary workers and other personnel who may access the internet through Company-issued devices or connect to the internet through the Company network.

4. Policy

4.1. Provision of Internet Access

4.1.1. The provision of internet access to employees is entirely at the discretion of the company, and may be reviewed and withdrawn at any time.

4.2. Acceptable Use

4.2.1. Internet privileges are granted to employees for the purpose of carrying out the business of the Company, and employees are expected to use the Internet primarily for the purpose of carrying out their job functions.

4.3. Personal Use

4.3.1. Employees are not entirely prohibited from personal use of the Internet, but personal use should be limited to minimal and incidental use.

4.3.2. All Internet access and activities are monitored and recorded by the Company's IT Department.

4.4. Prohibited Use

Prohibited use of the Internet on Company-issued devices or through the Company's network includes but is not limited to:

4.4.1. All types of hateful, discriminatory, offensive and violent content.

4.4.2. Access to Company documents and data that is not within the scope of the employees job duties.
4.4.3. Unauthorised use, misuse, disclosure, alteration, sharing or access of customer or personnel data or communications.
4.4.4. Linking of Company web content to Internet sites that contain content that is harmful, hateful, violent or otherwise inconsistent with the culture, values or policies of the Company.
4.4.5. Any Internet conduct that would constitute or encourage a civil or criminal offense, or otherwise violate any law or regulation in the jurisdiction or jurisdictions in which the Company operates.
4.4.6. Use, viewing, sharing or duplication of any material that infringes on copyrights, trademarks, trade secrets or patents of any person or organisation.
4.4.7. Transmission of any confidential, sensitive, personal or proprietary information without the proper authorisation or controls.
4.4.8. Creation, sharing, transmission, or voluntary receipt of any offensive, libelous, discriminatory or unlawful material including but not limited to material that discriminates on race, sex, gender, sexual orentiation, age, disability, religion, national origin or political beliefs.
4.4.9. Gambling and online gaming.
4.4.10. Dating and adult content.

4.5. Prohibited Activities

The activities are expressly forbidden:

4.5.1. Downloading, sharing or installing spyware, viruses, malware or any other type of harmful program or application.
4.5.2. Playing of any games.
4.5.3. Use of online dating services.
4.5.4. Forwarding of chain letters.
4.5.5. Viewing of pornographic or adult content.

4.6. Software License

4.6.1. Use or reproduction of software in a manner that infringes the vendor's license, copyrights or trademarks is forbidden.

4.7. Expectation of Privacy

4.7.1. The Company reserves the right to monitor all employee Internet activity, including Web activity, email contents and file downloads.
4.7.2. The Company cannot guarantee that any email other communications performed with the Company's Internet access will be private or confidential.

4.8. Maintaining the Company Image and Values

4.8.1. Employees must keep in mind that they are representatives of the company at all times. Whenever employees state an affiliation to the Company, they must clearly indicate that the opinions they may express are those and do not necessarily indicate the opinions or values of the company.

4.9. Company Materials

4.9.1. Company materials, data and communications may not be shared or posted publicly on the Internet without prior written approval by the employee's line manager and the Public Relations Department.

5. Policy Compliance

5.1. **Compliance Measurement**

The Infosec team will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. **Exceptions**

Any exceptions to this policy must be approved by the Infosec team in advance and have a written record.

5.3. **Non-Compliance**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Password Policy

1. Overview

Passwords are used to protect systems, data and devices across the business. Appropriate and secure use of passwords is essential for business security. Strong passwords significantly reduce the opportunity for unauthorised access to business information resources, whereas weak passwords heighten risks greatly.

2. Purpose

The purpose of this policy is to protect the company from the threats stemming from weak passwords and inappropriate use and sharing of passwords. These threats include loss of company data, tampering of company devices and systems, cost of recovering data, as well as the potential of regulatory fines.

3. Scope

The scope of this policy includes all employees, temporary workers, contractors and other personnel who use Company systems or devices or access the Company's data or network.

4. Policy

4.1. Password Creation

- 4.1.1. All passwords must conform to the Password Construction Guidelines.
- 4.1.2. A separate, unique password must be used for each separate account on the Company's devices, network or systems.
- 4.1.3. Passwords may not be reused for other applications within the Company or in personal use.
- 4.1.4. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, users should always use multi-factor authentication for accounts with system-level privileges when it is available.

4.2. Password Change

- 4.2.1. Passwords should be changed only when there is reason to believe that the password has been compromised.
- 4.2.2. Password cracking or guessing may be performed on a periodic or random basis by the IT team or approved delegates. If a password is guessed or cracked during one of these tests, the user will be required

to change it to be in compliance with the Password Construction Guidelines.

4.3. Password Protection

4.3.1. Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential information.

4.3.2. Passwords must not be inserted into email messages, texts or any other form of electronic or non-electronic communication, including over the phone.

4.3.3. Passwords may be stored only in “password managers” that have been specifically approved by the IT Department.

4.3.4. Any user suspecting that their password may have been compromised must report the incident and change the password as soon as reasonably feasible.

4.4. Multi-Factor Authentication

4.4.1. Multi-factor authentication is highly encouraged and should be used whenever possible, especially for systems that have access to sensitive data.

4.5. Application Development

4.5.1. Applications must support authentication of individual users, and to be able to function without any passwords having to be shared among users.

4.5.2. Applications must not store passwords in clear text or in any easily reversible form.

4.5.3. Applications must not transmit passwords in clear text over the network.

4.5.4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5. Compliance

5.1. **Compliance Measurement**

The Infosec team will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

5.2. **Exceptions**

Any exceptions to this policy must be approved by the Infosec team in advance and have a written record.

5.3. **Non-Compliance**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.