Unison Consulting Pte Ltd

Information Security Policy Unison Consulting Pte Ltd

1. Purpose

The purpose of this Information Security Policy is to establish a framework for managing and protecting the information assets of Unison Consulting Pte Ltd. This policy aims to ensure the confidentiality, integrity, and availability of sensitive information and to mitigate risks associated with information security breaches.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who have access to Unison Consulting's information systems and data. It encompasses all forms of information, including electronic, paper-based, and verbal communications.

3. Information Security Objectives

Confidentiality: Protect sensitive information from unauthorized access.

Integrity: Ensure that information is accurate and trustworthy.

Availability: Guarantee that authorized users can access information when needed.

All company resources must be protected and used responsibly and with care, for legitimate company business in accordance with the relevant policies in this section.

IT resources such as computer accounts, personal computers, servers, disk storage, software, email, network, internet and databases (collectively referred to as "IT Resources" are Unison Consulting property, and are for official Unison Consulting business purposes only).

4. Unison Consulting INTERNAL NETWORK ("NETWORK") SECURITY

4.1 NETWORK CONNECTION

Only Unison Consulting supplied or authorised computers shall be used to connect to the Network. Employees shall not:

- setup or install unauthorised wireless access points, on the Network.
- setup or host any server services (e.g. web server or file transfer servers, etc.) in the Network.
- connect their computers to publicly available networks via dial-up modems, mobile broadband devices and other connection devices while connected to the Network.
- allow third party vendors or consultants to connect their computers into the Network. If any network resource is required, e.g. internet, the Employee shall obtain approval from his supervisor, seek assistance from IT, and ensure that these third parties comply with this Policy.

4.1.2 UNAUTHORISED NETWORK ACTIVITIES

Employees shall not:

- access or attempt to access IT Resources that they are not granted access to.
- intercept or attempt to intercept data or communications not intended for them.
- scan Network or any IT Resources using hacking tools unless prior approval has been sought.
- impersonate or conceal computer network address.
- tamper with the IT Resources as that may potentially cause performance degradation, service instability, or compromise operation efficiency, security and fair use of resources.
- undermine the security of the IT Resources, e.g. to 'crack' passwords, modify or try to modify the files of other Board Directors or Employees or software components.

4.2 INTERNET USAGE

Use of the internet through or provided by the Network shall be for Unison Consulting connected work, although limited reasonable personal use is allowed.

Employees should note that communications on the internet are not automatically protected from viewing by third parties unless encryption is employed.

Employees shall not:

- issue search instructions and download content (e.g. video) manually or via automated agents that may consume large amount of network or internet bandwidth and IT Resources which may degrade the Network or IT system performance.
- save passwords in their web browsers or electronic mail clients, allowing automatic input for subsequent use.

4.2.1 PROHIBITED MATERIALS AND OTHER ONLINE / INTERNET ACTIVITIES

Employees shall not via the internet or Network:

- access, download, distribute, share or store materials that are obscene or pornographic, disrespectful, intimidating, slanderous or other materials that are unlawful onto Unison Consulting IT Resources.
- install and use peer-to-peer software (e.g. bittorrent, emule, web thunder) to share information or software
- play computer games and conduct gambling activities via the internet or Network.
- perform phishing, or other fraudulent activities using Unison Consulting IT Resources.
- perform audio/video chats or file transfers using internet messaging software.

4.3 INTELLECTUAL PROPERTY AND COPYRIGHT

Employees shall not download, repost, make copies, distribute or share any copyrighted materials or copyright infringing materials without prior permission from the copyright owner.

Employees shall ensure that there is no unauthorised disclosure of confidential information to any external party through the internet via any social medium

5. PASSWORD SECURITY

5.1 PERSONAL USER ACCOUNTS RESPONSIBILITY

Employees shall:

- be responsible for all activities performed from the accounts assigned to them.
- change passwords personally (no delegation to others), on first logon to, and whenever prompted by the systems.
- immediately change their password on any possibility of password disclosure or compromise.

Employees shall not:

- share or reveal any passwords or access codes under any circumstances.
- use easily guessed passwords, e.g. words, common character sequences, or personal details.
- store passwords in any easily accessed and readable forms e.g. post-it pads, electronic text files.

5.2 EMAIL SECURITY

5.2.1 EMAIL SYSTEM AND USAGE

Unison Consulting email system usage is for business purposes and personal use should be kept minimal. Employees shall:

- exercise care when sending out emails, to ensure the addressee(s) is/are the intended recipient.
- alert the author of any email not intended for them and to delete it promptly.
- periodically housekeep and purge emails that are no longer needed for business purposes.

Employees shall not:

- use their personal email accounts for any Unison Consulting business correspondences, or forward business email correspondences to personal email accounts or any external party without prior approval.
- delegate their email access to anyone.
- open email/attachment from unknown sources, as it may contain virus or other malicious wares.
- knowingly transmit any harmful or malicious content (e.g. viruses) or any other content that are obscene, racist, harassing, intimidating or otherwise that may violate the civil and criminal laws.
- use email for commercial solicitation, distribution of hoaxes, chain letter, or advertisements.
- forge the identity of or impersonate another person in an email.
- flood an individual, group or email systems with numerous or large emails.

6. DESKTOP/LAPTOP AND STORAGE DEVICE SECURITY

6.1 BUSINESS USE ONLY

Unison Consulting supplied personal computers and storage devices including thumb drives, hard disk drives, diskettes, CD-ROM (collectively "Storage Devices"), are for business use and should not be loaned to any third party (e.g. family members).

6.2 UNAUTHORISED CHANGES TO HARDWARE

Employees shall not on Unison Consulting supplied computers:

- alter the hardware configuration. Any required changes must be performed by authorised IT personnel.
- change the Operating System (OS) configurations.
- install non-work related software packages (e.g. games, or unlicensed/copyright protected software) and store illicit files. Any new installation for work related software package must be approved by the Employee's supervisor, then installed by authorised IT personnel.
- disable or uninstall security software enabled, e.g. antivirus.

6.3 VIRUSES, WORMS, TROJAN HORSES AND MALICIOUS CODE

Employees must not:

- attempt to eradicate any virus, worm, Trojan horse and/or malicious code (collectively "Viruses") without IT assistance. On suspicion of Virus infection on a computer or Storage Device, the Board Director or Employee must immediately stop using that device, physically disconnect from all networks, and call the IT Helpdesk for assistance.
- write, compile, copy, execute or attempt to introduce any computer code or Virus designed to self-replicate, damage, or otherwise hinder the performance of any Unison Consulting IT Resources.

6.4 PROTECTION OF COMPUTERS AND STORAGE DEVICES (AND INFORMATION CONTAINED WITHIN)

The following protection measures shall be undertaken by Employees:

- to lock their personal computer screens when leaving it unattended using Windows Screen Saver with password protection or by manually locking the screen (i.e. Ctrl-Alt-Delete); and to log-off from the network/systems at the end of day.

- protect Unison Consulting information on laptops and storage devices with the necessary safeguards (e.g. encryption, password protection).

- promptly inform their supervisor, if the equipment is damaged, lost, or stolen.

- disposal of computers and storage devices (e.g. hard-disk, floppy disks, CD, etc.), should be done with IT assistance to destroy, degauss, or overwrite these devices such that no information can be recovered.

Employees shall not:

- leave their laptops and storage devices unattended when out of the secure office areas.

- check-in laptops and storage devices in their luggage when travelling overseas.

- store Unison Consulting information locally on laptops, when bringing these on overseas trips. Information required should be retrieved via secure remote access channel (e.g. Citrix).

7. SYSTEM ACCESS CONTROL

Access to sensitive information will be governed by role-based access controls (RBAC). Employees will only have access to information necessary for their job functions.

7.1 SYSTEM ACCESS AUTHORISTATION

Employees are to note that access privileges are granted based on need-to-know basis, and they shall:

- promptly alert IT of any access that they have but should not be granted.

- inform IT to make relevant changes to access privileges on Unison Consulting production systems whenever there are any changes in end-user duties (e.g. change of department) or employment status.

- periodically determine (to be done by supervisors) whether current-enabled privileges, for production system that may have regulatory or financial impact to Unison Consulting (e.g. SAP, SUMMIT, Hyperion), are still needed by the relevant Employee to perform his current job duties. When such access is no longer necessary, the supervisor should promptly request IT to remove any excess privileges granted to the Employee.

Employees shall obtain formal authorisation for the following access requirements:

- all access requests for privileges and modifications of privileges on Unison Consulting production systems.

- remote access connection to the Network.

- temporary accounts for consultants, interns or temporary workers for project purposes.

Employees shall not deposit illicit files or programs on the file server (e.g. G and H drives).

Only administrative information should be stored on folders in computer systems to which Board Directors and/or Employees of other companies can access.

7.2 DATA BACKUP AND RESTORATION

Employees shall:

- save their working files on the file servers in directories reflecting respective business groupings (e.g. Finance, human resource) where periodic backing-up is done by automatic backup systems.

- obtain the necessary authorisation before restorations of data or information can be performed.

7.3 CHANGE CONTROL PROCESS

Employees shall note that:

- only after authorisation, should changes to any production system and data be effected.
- emergency changes may be applied to production environment after informal approvals (e.g. verbal approval) from the relevant approving parties; however, these changes and all approvals given have to be documented.

8. GENERAL

8.1 RIGHTS TO AUDIT

Unison Consulting through its representatives from the IT and/or appointed auditors reserve the right to perform security audits to ensure compliance.

8.2 ACCESS LOGGING AND MONITORING

Employees are to note that all system access and network related activities are logged. Unison Consulting or its representatives may access and monitor all aspects of the IT Resources under the following limited circumstances:

- For identification or diagnosis of systems, network or security vulnerability and problems;
- Where there are reasonable grounds to believe that there is a violation of law or a breach of Unison Consulting policies; or
- Where specifically allowed or required under the laws.

9. Roles and Responsibilities

Executive Management: Responsible for endorsing and supporting the implementation of this policy.

Information Security Officer (ISO): Oversees the development, implementation, and enforcement of the Information Security Policy.

Employees: Required to adhere to this policy and report any security incidents or vulnerabilities.

10. Data Classification

All data must be classified into categories based on sensitivity (e.g., public, internal, confidential, restricted). Appropriate security measures will be applied according to the classification level.

11. Training and Awareness

Regular training sessions will be conducted to ensure that all employees understand their responsibilities regarding information security. Awareness campaigns will promote best practices in protecting sensitive data.

12. Compliance and Legal Requirements

Unison Consulting will comply with all relevant laws and regulations concerning data protection and privacy, including the Personal Data Protection Act (PDPA).

13. Policy Review

This Information Security Policy will be reviewed annually or whenever significant changes occur in the organization or its operating environment to ensure its continued relevance and effectiveness.

Conclusion

The implementation of this Information Security Policy is essential for safeguarding Unison Consulting's information assets against threats and ensuring compliance with legal obligations. All personnel are expected to commit to these guidelines to foster a secure working environment.