Introduction

International Organization for Standardization (ISO) 27001 providing requirements for an information security management system (ISMS).

- Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

1.0 Acceptable Use 可接受的使用

1.1 General User and Ownership 一般用户和所有权

- TTC info must be protected
- report theft and loss to COO
- only can share TimeTec info after get authorized and use to fulfill job duties
- TTC may monitor computing devices,system & network for security purpose

1.2 Security and Proprietary Information

- System level & user level password must comply Password Policy, not allowed providing access to others
- All computer must log off after away
- Not allowed posting TTC employees email & address
- use extreme caution to open unknown email, which may contain malware

1.3 Unacceptable Use

- Violation of the rights, copyrights, trade secret, patent, pirated software is not appropriate licensed for use by TTC.
- Do not reveal passwords to others
- Do not make fraudulent offer on TTC products
- Do not introducing honeypots, honeynets, or similar technology on the TimeTec Cloud network.
- Do not Introduction of malicious programs into the network or server
- Do not providing information about, or lists of, TimeTec Cloud employees to parties outside TimeTec Cloud.

1.4 Email & Communication

- Sending unsolicited email messages,
- Any form of harassment
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Posting the same or similar non-business-related messages to large numbers via social media, newsgroups or forums.

1.5 Blogging and Social Media

- TimeTec Cloud’s trademarks, logos and any other TimeTec Cloud intellectual property may also not be used in connection with any blogging activity.
- If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of TimeTec Cloud.

2.0 Data Breach Response

2.1 Confirmed theft, breach or exposure of TimeTec Cloud data

- CTO analyze the breach or exposure to determine the root cause

2.2 Develop a communication plan.

- Human resource departments to decide how to communicate the breach

2.3 Ownership and Responsibilities

- IT Operation Team would provide administrative support for the implementation, oversight and coordination of security procedures

2.4 Enforcement

- Violation of this policy may be subject to disciplinary action, up to and including termination of employment and legal action. Any third party partner company found in violation, legal action may be instituted.

3.0 Bring Your Own Device (BYOD) Policy

3.1 Main Point

- To protect the security and integrity of TimeTec Cloud's data and technology infrastructure.

3.2 BYOD Acceptable Use

- Blocked from accessing certain websites (refer Employee Internet Use Monitoring and Filtering Policy)
- Can install any software/mobile apps (refer Software Installation Policy and Acceptable Use Policy)

3.3 Devices and Support

- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools,
before they can access the network.

3.4 Security

- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden
- Devices must be password protected using the features of the device and a strong password is required to access the company network in accordance with company's Password Protection Policy and Password Construction Guidelines

A. Devices may not be used at any time to:

Store or transmit illicit materials
Store or transmit proprietary information belonging to another company
Engage in harassment
Engage in outside business activities

3.5 Risks/Liabilities/Disclaimers

- Employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- Lost or stolen devices must be reported to the company within 24 hours.
- The company reserves the right to disconnect devices or disable services without notification.
- TimeTec Cloud reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

4.0 Email Policies

4.1 Main Point

- Email account should be used primarily for TimeTec Cloud business-related purposes;
- Personal communication is permitted on a limited basis, but non-TimeTec Cloud related commercial uses are prohibited.
- Email contained TTC business record must store at least 1 year in CRM
- Not storing privacy
- TTC able to monitor email
- Employees who receive any emails with inappropriate content from any TimeTec Cloud employee should report the matter to their supervisor immediately.

5.0 Employee Internet Use Monitoring and Filtering Policy

5.1 Internet Use Filtering System

- Block certain website

5.2 Internet Use Filtering Rule Changes

- IT operation team shall periodically review and recommend changes to web and protocol filtering rules

5.3 Internet Use Filtering Exceptions

- Employees may request the site be unblocked by submitting a request to the CTO. An IT Operation Team will review the request and unblock the site if it is mis-categorized.

6.0 Password Construction Guidelines

6.1 Strong passwords have the following characteristics

- Contain at least 8 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).

7.0 Password Protection Policy

7.1 Password Creation

- All user-level and system-level passwords must conform to the Password Construction Guidelines.
- Must not use the same password for TimeTec Cloud accounts as for other non-TimeTec Cloud access.

7.2 Password Change

- All system-level passwords must changed every 12 month
- All user-level passwords must changed every 6 month

7.3 Password Protection

- Do not simply send to others
- Do not put explicit hint
- Passwords must not be shared with anyone.
- Passwords must not be inserted into email messages, or other forms of electronic communication.
- Usage of "Remember Password" feature of applications (for example, web browsers) is not encouraged.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
- Where is available, it is recommended to use 2-Factor Authentication as an added security measure.

7.4 Application Development

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

For example: *Leave can apply leave on behalf of junior or subordinate.*

8.0 Removable Media Policy

8.1 Main Point

- Scan for virus/malware before use
- Encrypt sensitive data or files accordingly
- Cannot use in computer that not owned by TTC

9.0 Server Malware Protection Policy

9.1 Antivirus

- All servers SHOULD have an anti-virus application installed

9.2 Anti-Spyware

- All servers MUST have an anti-spyware application installed

UNLESS *it is a personal private server that only few people can use AND without connecting to the Internet OR it's Linux/Unix (non-Windows) based platform.*

10.0 Virtual Private Network (VPN) Policy

10.1 Main Point

- This policy is applicable to OpenVPN, IPSec, and L2TP
- Users of only company issued computers can have the access to the VPN facilities
- All computers connected to TimeTec Cloud internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard.

11.0 Remote Access Policy

11.1 Main Point

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.
- All hosts that are connected to TimeTec Cloud internal networks via remote access technologies must use the most up-to-date anti-virus software
- Personal equipment used to connect to TimeTec Cloud's networks must meet the requirements of TimeTec Cloud-owned equipment for remote access.

12.0 Database Credentials Coding Policy

12.1 Storage of Database Usernames and Passwords

- Database usernames and passwords may be stored in a file separate from the executing body of the program's code.

12.2 Retrieval of Database Usernames and Passwords

- If stored in a file that is not source code, then need to read it immediately, and clear the memory that contains the username and password after it is done use.
- The credentials must be in a separate source file.

12.3 Access to Database Username and Passwords

- Database passwords used by programs are system-level passwords
- Password need to follow password policy
- Can be set authentication for user

12.4 Developer Guide

https://docs.google.com/document/d/10QiiMceAV6z9vQAf9X459OAvPi6S2ak5s6d8QXrWWbM/edit

13.0 Software Installation Policy

13.1 Main Point

- May not install unauthorized software on TimeTec Cloud computing devices
- Software requests must first be approved by the HODs and then be made to the CTO in writing or via email.
- The IT Operation will obtain and track the licenses, test new software for conflict and compatibility, and permit the installation.

14.0 Technology Equipment Disposal Policy

14.1 Technology Equipment Disposal

- Technology assets have reached the end of their useful life and they should be sent to the IT Operation Team for proper disposal.
- Securely erase all storage
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

14.2 Employee Purchase of Disposed Equipment

- Equipment which is working, but reached the end of its useful life to TTC, will be made available for purchase by employees
- All equipment purchases must go through the HR, and they will determine the price.

15.0 Web Application Security Policy

15.1 Application Release

- Will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

15.2 Third Party or Acquired Web Application

- Will be subject to full assessment after which it will be bound to policy requirements.

15.3 Patch Releases

- Will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

15.4 Emergency Releases

- An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the CTO or an appropriate manager who has been delegated this authority.

15.5 Security Issues

- **High:** Any high-risk issue must be fixed immediately or may taken offline or denied
- **Medium:** need to schedule accordingly, or may taken off-line or denied release based on number of issues
- **Low:** need to schedule accordingly

16.0 Workstation Security Policy

16.1 Main Point

- Ensuring workstations are used for authorized business purposes only.
- Need to install antivirus software, except Linux/MacOS.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, on network servers or cloud storage.
- Keeping food and drink near workstations is not recommended.
- Securing laptops that contain sensitive information by locking laptops up in drawers or cabinets.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- If deemed necessary, all transmission of Confidential information through the internet must be encrypted or password protected.
- Transmission of Highly Confidential information through the internet is not permitted.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.

17.0 Information Asset Registry Guidelines Policy

Refer to the link, CLICK HERE