Cyber Security Policy

Revision 2

Cyber Security & Information Security

Prepared by: Paul Cutting

TPS | Total Peripheral Supplies Pty Ltd

Unit 3, 2 Garden Road
Clayton VIC 3168
Phone: (03) 9545 1266
Fax: (03) 9545 1288

Cyber Security Policy Approval and History Record

Revision Number	Description of Amendment and Reason for Change	Prepared / Reviewed by	Approved by	Date of Approval and Issue
1	Original approval and issue of the Cyber Security Policy	Paul Cutting	Rob Briede	23/05/2022
2	Amended version of SS policy	Paul Cutting	Rob Briede	15/07/2022

All revisions of this document are to be approved by the Finance and Compliance Manager and General Manager. Any requests for changes or additions should be made via email to the Finance and Compliance Manager and General Manager. Changes to this document will be recorded in accordance with TPSP 006 Documentation and Control.

Intent and Scope

The cybersecurity policy provides the basis of cybersecurity management within Total Peripheral Supplies (TPS).

This policy applies to all TPS employees, contractors, volunteers, vendors and anyone else who may have any type of access to Total Peripheral Supplies systems, software, and hardware.

Effective protection of business information creates a competitive advantage, both in the ability to preserve the reputation of TPS and in reducing the risk of the occurrence of negative events and incidents.

1.0 Roles & Responsibilities

Roles and responsibilities throughout the organisation are clearly defined in the organisation chart, however specific to cyber security management.

Rob Briede – GM – Manages the Cybersecurity Program,
David Gillies – MD – Takes organisation responsibility for the program,
Paul cutting – Finance & Compliance Manager – Responsible for program operation and SOE workstation environment,
Amanda Mystakidis – Project Officer – Responsible for dissemination of Cybersecurity information and certification of actions

2.0 Password requirements

To avoid employees, work account passwords being compromised, these best practises need to be followed for setting up passwords:

a. Use at least 8 characters (must contain capital and lower-case letters, numbers and symbols),
b. Do not write down password and leave it unprotected,
c. Do not exchange credentials when not requested or approved by your manager,
d. Change password every 3 months (or sooner if directed by alternate party such as Telstra).

3.0 Email Security

Emails can contain malicious content and malware. In order to reduce harm, employees shall employ the following strategies:

a. Do not open attachments (unless canned for viruses and from a known source),
b. Do not follow any links that are not well explained or expected. E.g. it would make sense to follow a link to the nab bank in an email from nab, but not in an email from an unknown source,
c. Check the email addresses and names of senders,
d. Search for inconsistencies,
e. Block junk, spam and scam emails,
f. Avoid emails that contain common scam subject lines such as prizes, products and money transfers.

4.0 SOE hardware & Software

TPS have provided a SOE computer (Toshiba Tecra) and SOE smartphone (iPhone). These devices will be issued to you by Paul Cutting. Any non-provided software and hardware accessories provided must not be used.

To enable use of non-provided software and hardware, please seek suitability assessment from Paul Cutting or the Cyber Security team so that approval for use can be granted.

5.0 Device Security and Using Personal devices

Logging into any work accounts for personal devices such as mobile phones, tablets or laptops, can put TPS data at risk. TPS does not condone accessing any TPS data from personal devices. However, if this cannot be avoided, employees are obligated to seek a specific exemption from a member of the cyber security team.

Employees must follow these best practise steps when using TPS devices:

a. Keep all electronic devices passwords secure and protected,
b. Logging into accounts should only be performed through secure networks,
c. Install security updates always,
d. Upgrade antivirus software on a regular basis,
e. Do not install software applications which are not provided by TPS,
f. Never leave devices unprotected and exposed,
g. Lock computers when leaving the desk.

6.0 Transferring Data

Data transfer is a common cause of cybercrime. Employees must follow these best practises when transferring data:

a. Avoid transferring personal information such as customer data and employee information,
b. Adhere to the relevant personal information legislation,
c. Data should only be shared by TPS approved methods (seek clarification from the Cybersecurity team or your manager),
d. If applicable, destroy any sensitive data when it is no longer needed.

7.0 Security Requirements

Employees must not install unauthorised software. The company may at any time introduce a whitelist of approved/trusted programs. If this occurs then only these programs may be used by employees.

Employees should perform daily backups of important new/changed data, software and configuration utilities.

Employees must not use unauthorised devices on their workstations, unless they have specific authorisation from TPS,

Employees must not attempt to turn off or circumvent any security measures.

Employees must report any security breaches, suspicious activities or issues that may cause a cyber security breach to TPS.

8.0 Shared Accounts

Each staff member is provided with a unique series of credentials to use for systems and physical security access (e.g. locks on doors). Staff must never share a credential to another employee. If approached by a colleague to share access, refer them to the General Manager for new credentials to be provided.

9.0 Disciplinary Action

If this policy is breeched, one or more of the following disciplinary actions will take place:

a. Incidents will be assessed on a case-by-case basis,
b. In the case of breaches that are intentional or repeated or in cases that cause direct harm to TPS, employees may face serious disciplinary action.
c. Subject to the gravity of the breach, formal warnings may be issued to the offending employee.