DOCUMENT No: TCCD-100117 | JULY 2024 | REVISION: 1

Cybersecurity Policy Suite

Contents

1 Purpose and application 3
2 Scope 3
3 Terms and Definitions 4
4 Responsibilities 5
5 Compliance with this Policy and Rights to Information 6
6 Relevant Procedures 6
7 IT Acceptable Use Policy 7
8 OT Acceptable Use Policy 8
Policy Details 9
Revision and Approval Details 10

1 Purpose and application

The purpose of this Policy is to offer clear guidance to employees and service providers on the appropriate, safe, and legal use of Company Information Technology (IT) and Operational Technology (OT). This guidance applies to Todd Corporation and its affiliated group companies, collectively known as “the Company”.

This Policy has been designed to align with and enhance the principles outlined in the NIST Cybersecurity Framework (CSF) 2.0, ensuring that the use of IT and OT within the Company adheres to industry cybersecurity standards.

2 Scope

This Policy applies to all employees and service providers and sets out the minimum requirements and expectations when using Company IT and OT.

IT security is dedicated to the protection of data and information integrity, while OT security is committed to the assurance of process safety and resilience.

The Company's IT environment, comprising systems, applications, and devices, is essential for daily operations, communication, and data management. Due to its network connectivity, it is vulnerable to cyber threats, necessitating robust security measures to protect data and ensure operational continuity.

The Company’s OT environment includes technology that oversees production plants, controls power generation stations, and manages utilities. OT is essential for the Company’s infrastructure, ensuring the availability and reliability of energy resources. Due to its critical nature and connectivity, the OT environment is at a heightened risk of cyber-attacks, which necessitates more robust security measures to protect against potential threats.

3 Terms and Definitions

Please refer to the glossary of terms for Policies on the Policy Centre. The following definition(s) are not in the glossary and are specific to this Policy:

Term	Definition
Chief Information Security Officer (CISO)	The executive responsible for the Company's IT and OT security. Position held by the Group Manager Technology & Security.
Information Technology (IT)	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, which are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Examples include Company issued devices and Company licenced applications such as Microsoft 365, TechnologyOne, Salesforce etc.
Operational Technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include Safety Instrumented Systems (SIS), process control systems etc.
Technology & Security Team	The team responsible for IT and OT security at the Company.
Technology & Security Service Desk	A centralised support function that provides a single point of contact within the Company to manage and resolve IT related issues, service requests, and inquiries. The portal can be found here: https://toddcorporation.freshservice.com/support/home
Service Providers	An entity or individual that is trusted by the Company to provide certain services.

4 Responsibilities

Who	What you must do
All Employees and Service Providers	• Read this Policy prior to using Company IT and / or OT. • Complete training as outlined by this Policy. • Adhere to the acceptable use requirements detailed in this Policy. • Report breaches of this Policy to your line manager / supervisor, People & Culture, or the Technology & Security Service Desk.
CISO	• Review and update the Policy annually to confirm it is fit for purpose. • Enforce the Policy and manage breaches to this Policy if they occur. • Provide reporting to the Executive Committee (ExCom) and the Board.
Company Managers / Supervisors	• New employees and service providers are to be given a copy of this Policy upon commencement. • Ensure direct reports comply with the Policy. • Promote awareness of this Policy.
Technology & Security Team	• Monitor compliance. • Provide training and raise awareness. • Respond to breaches.

5 Compliance with this Policy and Rights to Information

Summary	Detail
Compliance	Any use of Company IT / OT which breaches this Policy may be classified as misconduct or serious misconduct under the Code of Conduct, and may be subject to disciplinary action, up to and including dismissal. Your IT or OT access may be suspended pending an investigation, disciplinary action, or termination of your employment. For the definition and consequences of misconduct and serious misconduct, refer to the Code of Conduct.
Reporting Non-Compliance	An employee or service provider who fails to follow this Policy will not be meeting their obligations under the Code of Conduct. If an employee or service provider observes or suspects an instance of unacceptable use, they should report that immediately to a line manager / supervisor, People & Culture representative, or Technology & Security Service Desk. An employee or service provider who knows of a failure to comply with this Policy or the Code of Conduct and who fails to report the non-compliance may also be subject to disciplinary action. Serious wrongdoing should be reported in line with the Code of Conduct.
Rights to Access Information	All data and information on Company IT / OT is the property of the Company, subject only to relevant regulations and contracts. The Company retains the right to access and audit all Company IT / OT and all data, information, and activity on Company IT / OT and monitor use at any time without seeking an employee's specific consent. This may include personal use, including after-hours internet use from a Company site or a Company IT device. The Company retains the right to remove any data / information on Company IT / OT at any time without seeking the employee's specific consent.
Rights to Disclose Information	The Company retains the right to request other companies or authorities to perform monitoring, access and/or audit on behalf of the Company. The Company may disclose the details of monitoring and audit findings, which will be managed by the People & Culture or Legal functions if required. The Company may provide logs and evidence of employee activity to law enforcement and Government security agencies to support its security objectives and investigations into illegal activity.

6 Relevant Procedures

The Technology & Security section within the Group Policy Centre contains the Procedures designed to support the Company in achieving the objectives of this Policy.

7 IT Acceptable Use Policy

IT* Acceptable Use Policy

This Policy applies to all employees and service providers and sets out the minimum requirements and expectations when using Company IT.

Acceptable Use

Take care of your Company issued devices and promptly report any incidents of damage or loss.

- You are personally responsible for looking after Company devices allocated to you and for ensuring the security of these devices.
- If you have a Company issued phone or laptop, take it home with you to ensure business continuity.
- Only you can use your Company issued devices. No one else can use it at any time.
- If your Company issued device is not fit for purpose, return it to the Technology & Security Team.
- You must report the loss, theft, or damage of Company IT assets to your manager / supervisor or the Technology & Security Team as soon after the event as possible.
- At the end of your employment / contract, you are required to return all Company issued devices.

Use a unique password and a second factor of authentication if available.

- Every employee is provided with an individual account and you must never use another employee's account.
- Use a secure password and an additional factor of authentication for your account when available.
- Don't share passwords or additional factors of authentication with other employees.
- Don't use the same passwords for work and personal accounts.

Personal devices may be used for Company purposes provided they meet certain requirements.

- They only connect to Guest networks in Company offices.
- M365 applications can be installed but Company Confidential or Company Personal Information (PI) must not be stored on personal devices / storage services.

Ask your manager / supervisor or the Technology & Security Team about which applications to use.

- You must use only approved applications and cloud services for work related tasks. If there's any uncertainty consult your manager / supervisor or the Technology & Security Team.
- If you can't find what you need, make a request to the Technology & Security Service Desk.

Please report any security breaches or concerns.

- Immediately report any unauthorised access, suspicious activity, or cybersecurity incidents to ensure the safety and confidentiality of our Company IT and OT.

Stay up to date with all required security training.

- You are required to complete annual acceptable use training.
- You may be asked to complete additional cyber training modules to mitigate risks associated with the dynamic nature of cyber-attacks.

Company issued devices are managed and monitored, and must be used responsibly.

- Company devices and IT systems are managed and monitored by the Company.
- The use of Company devices and IT systems must adhere to all applicable laws, align with Company policies, and safeguard the Company from any risks.
- The Company reserves the right to monitor and delete personal data and information on its devices and IT systems as per its policy and legal regulations.
- Company devices may be utilised for personal purposes, as long as such use does not impede work duties, diminish job performance, or conflict with professional responsibilities.
- Do not sign up for personal services or subscriptions using your Company provided email address.
- A Company mobile phone and mobile phone plan are primarily for business purposes. Reasonable personal use is allowed provided it does not incur additional cost.
- International calling, global roaming, and paid text services must only be for business purposes.
- All purchases of additional data packs and roaming services for business travel must have prior approval from your line manager / supervisor.
- The Company may charge you for any additional costs incurred due to personal use.
- You may keep the mobile number from your Company phone, if approved, to use it as your personal number after you leave the Company.

***Information Technology (IT):** Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Examples include Company issued devices and Company licenced applications such as Microsoft 365, TechnologyOne, Salesforce etc.

Prohibited Use

Don't let anyone else use your Company issued devices.

- Company devices are assigned for employee or service provider use only.
- Do not allow family members, friends, or other colleagues to use these Company devices.
- Misuse by others can lead to disciplinary action against the Company device's assigned owner.

Don't share your account and/or password with anyone, including other employees.

- Avoid writing down passwords where others can find them.
- Refrain from using the 'Remember Password' feature on shared devices.
- Never disclose your password in response to an email, phone, or chat request.

Don't use unapproved cloud applications and storage, or attempt to install unapproved applications.

- Don't sign up to, or store data on, unapproved cloud services.
- Don't attempt to download or install unapproved applications.
- If you can't find what you need, make a request to the Technology & Security Service Desk.
- Respect any restrictions on application or cloud service use imposed by the Company for security and compliance reasons.

Don't plug in unapproved USB devices.

- Only use Company approved USB devices to store or move data.

Don't try and circumvent our security controls.

- Don't try to circumvent our security controls, they are there to protect the Company.
- Adhere to the Company's Technology & Security policies and be vigilant when it comes to IT and OT security, risks, scams and emails from unverified or unknown senders.

Exceptions

- The Technology & Security Team may allow or deny a particular prohibited use to any employee based on appropriate risk analysis, risk management and business justification, and they may revoke this right at any time.
- Requests to use Company IT or Non-Company IT in exemption from this Policy must be submitted to the Technology & Security Service Desk.

Compliance

- Any use of Company IT which breaches this Policy may be classified as misconduct or serious misconduct under the Code of Conduct, and may be subject to disciplinary action, up to and including dismissal.

8 OT Acceptable Use Policy

OT* Acceptable Use Policy

This Policy applies to all employees and service providers and sets out the minimum requirements and expectations when using Company OT.

Acceptable Use

- Only use Company devices provided specifically for the OT environments.
  - Do not use Company provided IT devices on OT networks.
  - Employees and service providers must not bring any IT equipment onsite and connect it to the OT environment.
- Give your Company OT device back before you leave site.
  - When leaving site(s) you must hand back all Company OT devices.
  - Company OT devices are not to be used in any other environments or connected to the Internet.
- Shared OT passwords for commissioned technology must be stored in the site password vault.
  - Passwords must meet the complexity requirements defined by the Company and be unique for each system.
  - Inform the Technology & Security Team if any new account is created, identified, or hardcoded into any OT system or service.
- Stay up to date with all required OT security training.
  - All employees and service providers accessing Company OT are required to complete the Company specific site induction and the OT acceptable use training module.
  - You may be asked to complete additional OT cyber training modules to mitigate risks associated with the dynamic nature of cyber-attacks.
- Support additional vetting and proof of competencies.
  - With changing legislative requirements, and increased risk, the Company may at any time vet or require proof of competency for any employees or service providers working in Company OT environments.

Note

- While the IT Acceptable Use Policy remains applicable to OT environments, the OT Acceptable Use Policy will take precedence to accommodate OT's unique operational and security requirements.

***Operational Technology (OT):** Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include Safety Instrumented Systems (SIS), process control systems etc.

Prohibited Use

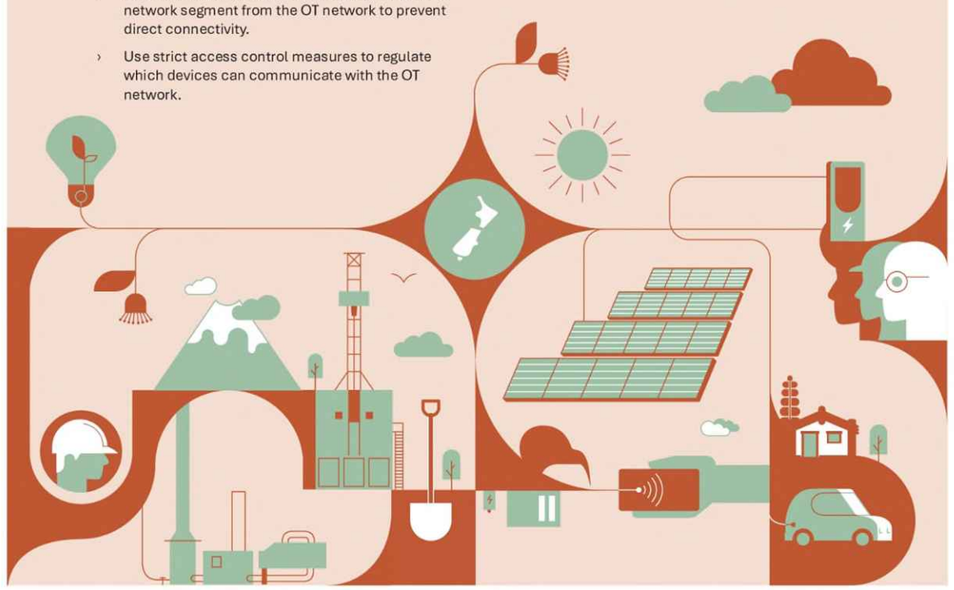
- No personal use is allowed on Company OT.
  - Do not connect personal devices, such as laptops or tablets, to the Company OT networks.
  - Ensure that all activities conducted on the Company OT systems are strictly related to operational activities and tasks.
- No default manufacturer or third party credentials may be used on Company OT.
  - No manufacturer or third party default credentials may be used for Company OT.
  - Don't use the same passwords for IT, OT and/or personal accounts.
- Don't make any changes to Company OT without following Management of Change (MoC) procedures.
  - All changes on Company OT (including patching, account or configuration changes) must be logged, assessed and approved before being executed.
- Industrial Internet of things (IIoT) and Internet of Things (IoT) devices cannot be directly connected to OT networks.
  - Ensure that IIoT and IoT devices are on a separate network segment from the OT network to prevent direct connectivity.
  - Use strict access control measures to regulate which devices can communicate with the OT network.

Exceptions

- The Company may allow or deny a particular prohibited use to any employee or service provider based on appropriate risk analysis, risk management and business justification, and they may revoke this right at any time.
- Requests to use Company OT devices in exemption from this Policy must be submitted to the site engineers or the Technology & Security Service Desk.

Compliance

- Any use of Company OT which breaches this Policy may be classified as misconduct or serious misconduct under the Code of Conduct, and may be subject to disciplinary action, up to and including dismissal.



Policy Details

Document title
IT & OT Acceptable Use Policy
Policy group
Technology & Security
Related policy documents
Code of Conduct Cybersecurity Policy Suite Privacy Standard Risk Policy Technology Governance Policy
Document owner
Group Manager Technology & Security
Document author
Group Manager Technology & Security