Cybersecurity Policy Suite

Document No: TCCD-100117

Revision: 0

July 2024

The Todd Corporation, 95 Customhouse Quay, PO Box 3142 Wellington 6140 New Zealand
P +64 4 472 2970

Contents

1 Purpose

The purpose of this Cybersecurity Policy Suite is to strengthen cybersecurity resilience by adopting the NIST Cybersecurity Framework (CSF) 2.0. Designed to manage cyber risks and protect digital assets, this Policy Suite is key in aligning our cybersecurity measures with the broader enterprise risk management strategies. It ensures compliance with relevant regulations and is applicable across Todd Corporation and its associated entities, collectively referred to as “the Company”.

2 Scope

This Cybersecurity Policy Suite, and associated policies, is relevant for all Company entities and applies to both Information Technology (IT) and Operational Technology (OT) environments.

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 are specific to this Policy.

Definition	Term
Chief Information Security Officer (CISO)	The executive responsible for the Company's IT and OT cybersecurity. Position held by the Group Manager Technology & Security.
Cybersecurity Event	A cybersecurity change that may have an impact on organisational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	An occurrence that (1) actually or imminently jeopardises, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Data Asset	Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset.
Digital Asset	Any asset that is purely digital or is a digital representation of a physical asset.
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.
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 cybersecurity.
Service Providers	An entity or individual that is trusted by the Company to provide certain services.

4 Responsibilities

Who	What you must do
CISO	• Establish the organisation's cybersecurity vision and align it with business goals. • Craft and update cybersecurity policies to address cybersecurity risks. • Identify, evaluate, and mitigate risks across IT and OT systems. • Ensure adherence to legal, regulatory, and internal policy requirements. • Communicate the importance of cybersecurity to stakeholders and maintain transparency in cybersecurity matters. • Lead the preparation for and response to cybersecurity incidents. • Develop and promote cybersecurity awareness and training programs. • Collaborate with internal and external stakeholders to maintain cybersecurity policies and procedures. • Allocate resources effectively to maintain and improve cybersecurity measures. • Establish and monitoring key performance indicators to measure the effectiveness of cybersecurity initiatives. • Regularly review and enhance cybersecurity strategies and processes.
Company CEOs (or Delegates)	• Demonstrate a strong commitment to cybersecurity and set clear expectations for cybersecurity practices. • Allocate adequate resources to support cybersecurity initiatives and maintain robust cybersecurity measures. • Actively participate in cyber risk management and integrate cybersecurity into the company's overall risk management strategy. • Foster a culture of cybersecurity awareness and responsibility at all Company levels. • Champion ongoing cybersecurity training and awareness programs for all employees. • Ensure the organisation has a well-defined and tested Incident Response (IR) and Disaster Recovery (DR) plans. • Communicate the importance of cybersecurity to stakeholders and maintain transparency in cybersecurity matters. • Stay informed about and ensure compliance with relevant cybersecurity laws, regulations, and industry standards. • Encourage regular reviews and updates of cybersecurity policies and practices to adapt to changing threats and technologies.
All Employees and Service Providers	• Ensure compliance with the Cybersecurity Policy Suite. • Identify and manage risks related to Company IT and OT cybersecurity.

Who	What you must do
Technology & Security Team	• Enforce cybersecurity policies across all technology platforms. • Conduct regular threat assessments and update defensive measures. • Manage the day-to-day operations of cybersecurity systems and infrastructure. • Lead the technical response to cybersecurity events and incidents. • Provide cybersecurity training and technical support to Divisions. • Oversee identity and access management across all systems. • Conduct audits to ensure compliance with internal and external regulations. • Keep cybersecurity technologies up-to-date with the latest protections. • Work with stakeholders to understand their cybersecurity needs and ensure that cybersecurity measures align with business objectives.

5 Compliance with this Policy

Breaches of the policies outlined in this document will be regarded in the same manner as other instances of misconduct within Todd. Allegations of improper behaviour will be assessed following the established protocols in the code of conduct policy. Penalties for failing to comply may encompass, but are not limited to, a range of consequences including:

1. Disciplinary action.
2. Termination of employment.
3. Legal action according to applicable laws and contractual agreements.

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 Cybersecurity Policy Suite.

7 Cybersecurity Policy

7.1 Purpose

The purpose of this Policy is to define the Company's approach to managing cybersecurity risks and protecting IT and OT environments. Effective cybersecurity policy and management will enable:

a) Improved cybersecurity risk identification and compliance.
b) Reduced potential of harm due to a cybersecurity incident.
c) Reduced service disruption and cost related to cybersecurity incidents.
d) Improved reporting and metrics for cybersecurity and related investments.

7.2 Principles

To effectively manage cyber risks and safeguard IT and OT environments, each entity within the Company is required to comply with the following principles**:**

a) Cybersecurity risks associated with IT, OT, service providers, and supply chains are systematically identified and prioritised in alignment with the Company's context, strategic objectives, and business imperatives.
b) All pertinent cybersecurity related compliance obligations, regulatory mandates, and legislative directives for IT and OT environments are thoroughly catalogued and observed.
c) IT and OT configurations employ cybersecurity methodologies and controls that are aligned with the NIST 2.0 Cybersecurity Framework (CSF) and the Company's defined risk appetite.
d) Continuous monitoring of cybersecurity risks, vulnerabilities, and potential indicators of compromise is maintained across IT and OT.
e) Employees and relevant service providers are provided with adequate cybersecurity training and are kept informed about all pertinent Technology & Security policies.
f) The effectiveness of cybersecurity controls is validated using a robust risk-based approach.
g) The Company has appropriately trained cybersecurity resources.
h) Cybersecurity Incident Response (IR) plans are maintained and tested.
i) Any exceptions to Technology & Security policies must follow the appropriate exemption procedure.

8 Data Asset Policy

8.1 Purpose

The purpose of this Policy is to define the Company's approach for managing data assets. Effective data asset management will enable:

a) Improved accountability for maintaining the confidentiality, integrity, and availability of data assets.
b) Reduced data assets cybersecurity and privacy risks.
c) Consistent compliance with regulatory and legislative requirements.
d) Reduced costs for sharing and managing data assets over their full lifecycle.

8.2 Principles

To effectively manage cyber risks and safeguard data assets, each entity within the Company is required to comply with the following principles**:**

a) Data assets are classified based on the requirements for confidentiality, integrity, and availability.
b) Protection measures are aligned with the data assets classification level.
c) Designated roles exist who are responsible for data assets and ensure Policy compliance.
d) Management, storage, sharing, and access to data assets comply with relevant legal and regulatory standards.
e) Data assets are only stored, shared, and accessed exclusively through approved systems and methods.
f) Specific retention periods are established and maintained for each data assets system or source.
g) Data assets are securely disposed of when it reaches the end of its lifecycle.

9 Asset Management Policy

9.1 Purpose

The purpose of this Policy is to define the Company's approach for the governance of IT and OT assets, collectively referred to as "assets", across their full lifecycle. Effective asset management will ensure:

a) Streamlines the identification and remediation of affected assets, minimising the impact and duration of cybersecurity incidents.
b) Reduced service disruption due to equipment or system failure.
c) Increased oversight of asset maintenance requirements and costs.
d) Improved vulnerability management which reduces cybersecurity exposure.
e) Improved asset lifecycle management.

9.2 Principles

To effectively manage cyber risks and safeguard assets, each entity within the Company is required to comply with the following principles**:**

a) Every asset is catalogued within the designated asset management systems for both IT and OT.
b) Periodic asset discovery exercises must be conducted regularly to identify assets not yet documented in the necessary asset management systems.
c) Records of assets are complete and contain all required attributes.
d) Ownership of assets is clearly defined and recorded, ensuring accountability and proper stewardship.
e) Assets are categorised following the Company's asset management lifecycle protocols.
f) Digital assets must be protected in accordance with the Cybersecurity Policy and associated procedures.
g) Access to assets is provisioned according to the Identity and Access Management Policy.
h) End-of-life hardware is securely disposed of when it reaches the end of its lifecycle.

10 Identity and Access Management Policy

10.1 Purpose

The purpose of this Policy is to define the Company's approach for managing digital identities and system access within IT and OT environments. Effective identity and access management will ensure:

a) Meeting legal and regulatory requirements.
b) Reduced risks of unauthorised access to IT and OT.
c) Employees and service providers have appropriate access to IT and OT.
d) Accurate and timely reporting on access rights and usage for audit integrity.

10.2 Principles

To effectively manage cyber risks and safeguard digital identities, each entity within the Company is required to comply with the following principles**:**

a) Access rights are granted based on the minimal level of privileges necessary, with distinct separation of duties tailored to each role.
b) System access in IT and OT environments must be authenticated against the Company's identity provider.
c) Accounts belonging to employees and service providers with fixed-term agreements are assigned explicit expiration dates.
d) A unique identifier is allocated to each employee, service provider, device, and process to ensure traceability.
e) System access is requested and approved by appropriate parties prior to being granted.
f) System access is reviewed periodically.
g) The use of shared accounts within the IT environment is strictly prohibited.
h) The sharing of personal passwords and other sensitive credentials in the IT environment is expressly forbidden. Administrative passwords must include measures to mitigate risks associated with the necessary sharing of credentials within the Technology & Security team, ensuring secure and controlled access.
i) Default system, device, and account passwords must be promptly replaced with strong, unique alternatives.

11 Change Management Policy

11.1 Purpose

The purpose of this Policy is to define the Company's approach for managing digital change within IT and OT environments. Effective change management will enable:

a) Operational continuity and reduce disruption during change.
b) Mitigate cybersecurity risks by implementing controlled and reviewed changes
c) Improved visibility of the Total Cost of Ownership (TCO) for IT and OT.
d) Reduced costs by standardising change methods, architecture, and support.

11.2 Principles

To effectively manage cyber risks and ensure aligned digital change, each entity within the Company is required to comply with the following principles:

a) All system changes must adhere to an established Management of Change (MoC) process.
b) Any new systems or solutions require evaluation and formal approval by responsible Company person.
c) Changes to production systems require an impact assessment addressing potential effects on system interdependencies, cybersecurity posture, architectural integrity, training needs, communication strategies, and overall system resilience.
d) Changes must undergo testing in existing test environments to ensure quality and performance. In the absence of such environments, changes should be carefully validated through alternative verification methods to maintain system integrity.
e) All changes must be requested, recorded and submitted through the approved IT or OT environment system.

12 Response and Recovery Policy

12.1 Purpose

The purpose of this Policy is to establish protocols for managing digital backups, recovery operations, and Incident Response (IR) within IT and OT environments to ensure Company resilience and continuity. Effective response and recovery will enable:

a) Reduced operational downtime, service disruption, and data loss.
b) Reduced impact due to a major incident.
c) Increased business resilience against incidents.
d) Reduced cost of response for incidents.
e) Improved productivity and communication to key stakeholders and staff during incidents.
f) Increased data retention capabilities for investigations, regulatory requirements, and business intelligence.

12.2 Principles

To effectively manage cyber risks and ensure recovery post incident, each entity within the Company is required to comply with the following principles**:**

a) Establish a strategic framework for Disaster Recovery (DR) that encompasses all services and systems, including those provided by external entities, to ensure resilience and tailored recovery strategies.
b) Implement a robust backup strategy that aligns with the strategic DR framework, ensuring the integrity and availability of all critical systems.
c) Formulate detailed DR plans for all critical systems, outlining clear recovery steps and responsibilities.
d) Conduct regular tests of backups and DR plans to maintain effectiveness and currency.
e) Maintain backups and DR plans in a secure environment, ensuring they are readily accessible in case of a major cybersecurity incident or system outage.
f) Ensure the availability and readiness of resources, including personnel, to execute DR plans effectively, as part of the Company's commitment to recovery readiness.

To effectively manage cyber risks and ensure response during incidents, each entity within the Company is required to comply with the following principles**:**

a) Incident Response (IR) capabilities must be in sync with Disaster Recovery (DR) requirements to ensure a cohesive approach.
b) Implement a Company-wide framework for incident prioritisation and response initiation, reflecting the Company's risk posture and business continuity objectives.
c) Develop an IR plan that is integrated into the company's risk management and business resilience strategies.
d) Enforce a protocol for responding to incidents based on their impact on the company's operations and assets, ensuring a swift and effective resolution.
e) Ensure comprehensive documentation of IR activities to support accountability, learning, and compliance.
f) Implement a system for tracking and analysing incidents to inform risk assessments and continuous improvement efforts.

13 Digital Cybersecurity Awareness Policy

13.1 Purpose

The purpose of this Policy is to define the Company's approach to fostering a culture of digital cybersecurity awareness. Effective digital training and awareness will enable:

a) Decreasing the frequency of cybersecurity events and incidents.
b) Shortening the duration from incident detection to resolution.

13.2 Principles

To effectively manage cyber risks and increase digital cybersecurity awareness, each entity within the Company is required to comply with the following principles:

a) A Company-wide digital training and awareness programme will be made available to all employees and relevant service providers. This needs to align with the latest cybersecurity trends and threats.
b) A periodic IT and OT acceptable use training program must be developed to ensure the minimum requirements and expectations when using Company IT and OT are understood. This is required to protect Company IT, protect Company OT, and reduce legal risks.
c) Enhanced training and awareness programs must be developed for roles targeted by cyber adversaries and those working in OT environments.

14 Policy Details

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

Revision and approval details

Revision	Published Date	Reason for Issue	Author	Reviewer	Reviewed Date	Approver	Approved Date	Document Initiated
	15/07/2024 10:05:27 AM		James Blair	Neil McKay;Adam Tapsell	2/07/2024 12:00:00 AM	Evan Davies	15/07/2024 9:59:45 AM	28/03/2024 11:12:07 AM