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.

TODD CORPORATION

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.