

# Customer ICS OT Security Program Governance Committee Charter

## Purpose

---

To create both executive level and technical expert level councils to guide the improved mature of security for industrial automation, instrumentation and control systems in use throughout Customer mills, buildings, facilities, utilities, plants and other locations. To ensure the ICS OT security program aligns with uniform goals mapped to relevant international standards for safety and security engineering of control systems. To ensure matrixed collaboration and dotted line reporting lanes for information sharing, funding of tools, resources and training are strategically decided and controlled consistently across all Customer businesses, units and locations.

## Type of Committee

---

Permanent standing committee that meets (monthly) to determine, manage, update and maintain Customer strategic executive and technical governance security goals, objectives, requirements for ICS OT security across all company buildings, facilities, utilities, mills, plants, operations equipment etcetera.

## Membership

---

### Executive Council level

CISO

CSO

VP of Safety

VP of Pulp

VP of Solid Wood

Mill Managers (one for pulp, one for solid word, one for US, one from Canada)

VP of HR

## Technical SME Council Level

CISO

Enterprise IT Security Lead (support for IT level functions)

ICS Security Managers (including regional managers)

Plant Safety Manager

Facilities, Utilities & Maintenance Lead/Engineer

Quality Lead Engineer

Plant Control Systems Engineering Leads

Plant ICS Security Engineer Leads

Plant Physical Security Leads

Plant level HR SME

## Roles & Responsibilities

---

**Chairperson(s) (CISO, CEO, CSO etc)** – will lead, champion, convene, manage, steer and facilitate the overall committee both executive and technical levels councils. Will also ensure that the technical council's technical requirements and implementation decisions and guidance stays in alignment with overall strategic ICS OT security standards and company maturity goals. Select the correct ICS OT security and safety international standards, trainings and certifications needed to improve capabilities and maturity of the company.

**Operational and Support SMEs Executive council level** – to provide accountability, staffing, funding, support for ICS OT security training and certification of staff under their purview to support matrixed collaboration of ICS OT security mission.

**Operational and Support SMEs Technical council level** – to ensure ICS OT security specifications, tools, requirements, personnel, suppliers, etcetera stay in alignment with selected ICS OT security standards, policies and procedures. To ensure they obtain, maintain and assign local personnel with the proper ICS OT security standards and certifications (e.g. GICSP and ISA/IEC 62443, ISA84) and to put those designated employees forward to the Executive level council for funding, staffing support, alternates and matrixed cross training needs at technical and field operations levels.

## Activities and Duties

---

What work will the committee do during meetings and between meetings. What will Exec level plan and decide then assign to tech level SME council etc? What will be done between monthly meetings?

### Executive Council

- Determine short, mid and long-term strategic organizational goals for ICS OT Security

- Determine initial ICS OT security policies, procedures, international standards, certifications and trainings needed
- Determine and agree on matrixed staffing, funding, collaboration and information sharing rules of engagement
- Ensure the proper technical leads and subject matter experts are assigned to the technical council with alternates and coverage across US, Canada and different businesses (e.g. Pulp, Solid Wood etc)

## Technical Council

- Ensure all appropriate technical staff receive the support, training, certifications and tools needed to implement and comply with ICS OT security standards, policies, procedures and strategic goals of company
- Lead and manage technical implementation, testing, validation, verification, maintenance and continuous reporting of ICS OT security functional security and safety requirements, tools, procedures, manuals, practices etcetera.
- Ensure third party staff complies and supports all ICS OT security and safety requirements, procedures, policies and standards
- Act as subject matter experts and mentors to all staff within their region, mill, departments, contractors and third parties etcetera
- Remain current on latest and greatest updates to ICS OT security standards as well as tools and attacker behaviors targeting ICS OT assets, systems, personnel, vendors, suppliers, integrators etcetera.
- Be mindful of and report insider threats and create a culture where full disclosure of mistakes are documented and encouraged and met with support and additional training rather than punishment for actions that were not intentionally malicious.
- To lead by example in a culture of safety and security for ICS OT assets, personnel, sites and operations

## Delegation of Authority

---

Define decision that can be made, number of votes needed, primary reps that must be present for vote to count (e.g. CISO, VP of Ops etc) and what decisions can be made without formal votes etc (e.g. CISO-Chair can make the call as agreed in charter by all executive level council members), reporting to company board and CEO, authority of committee etc.

## Committee Procedures

---

Frequency of meetings, location or tools of meetings, ad hoc and emergency of meetings, format, meeting minutes, assigning alternates when primary member is unable to attend, topics/agenda, updates/reporting, assigning of action items etc

## Executive Signatures and Signoffs

---

CISO

CSO

VP of Safety

VP of Pulp

VP of Solid Wood

Mill Managers (one for pulp, one for solid wood, one for US, one from Canada)

VP of HR