CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Cybersecurity Program Charter

Establishes the operational technology (OT) cybersecurity program for [Company Name], built on NIST SP 800-82r3, NIST CSF 2.0 and ISA/IEC 62443.

Organization	[Company Name]
Document ID	OT-01
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Write this with the Plant Manager and Health & Safety. An OT program without operations' support will fail.
- List every site and the main control systems in scope. Unknowns are fine at first; the 90-day plan finds them.
- Set a realistic maturity target (section 6). Most first-year programs aim for Maturity Level 2 on the core practices.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Mar 2023	The EU cybersecurity agency's study of transport incidents (Jan 2021 to Oct 2022) found ransomware was the most prominent threat (38%), that most attacks hit IT systems but still disrupted operations, and that ransomware groups are likely to target OT.	Most attacks start in IT and spill into operations, so mandate (section 4) must cover the IT/OT boundary.

Summarized by CyberGlass from public reporting: Public reporting summarized on Wikipedia, Oct 2025; Public ICS security reporting, 2017–2018; ENISA Transport Threat Landscape, Mar 2023. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
OT-03 Governance Framework	IT/OT Steering Committee, management of change, supplier rules
OT-04 Policy	Approved under this charter
OT-07 Strategy and Roadmap	Turns section 6 objectives into a funded 24-month plan
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Objective 3 'all remote access via jump host with MFA' → remote path RA-07 found in the workbook with a vendor modem → risk R-004 → closed when the modem is removed (evidence: photo and firewall rule).

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT First 90 Days Plan

A safe, practical 30-60-90 day plan for a new OT security lead at [Company Name], following NIST SP 800-82r3 and ISA/IEC 62443.

Organization	[Company Name]
Document ID	OT-02
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- The first month is about trust. Spend time on the plant floor before proposing changes.
- Never run active network scans or install tools on control networks without operations' written approval.
- Schedule any security changes inside planned maintenance windows.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

How this document connects

Document or register	How records and decisions flow
OT-08 Assessment Toolkit	Interview questions and evidence checklist for days 1–30
OT-10 Shop Floor Checklist	First walk-through in days 1–30
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Walk-through (OT-10) finds a cellular modem in a PLC cabinet → remote path RA-03 → removed in days 31–60 → KPI 'standing vendor connections' drops from 4 to 1.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Cybersecurity Governance Framework

How OT cybersecurity decisions are made jointly by operations, engineering, safety, IT and our service providers at [Company Name].

Organization	[Company Name]
Document ID	OT-03
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Make sure operations and safety have real decision rights; otherwise the framework won't be followed.
- Link security changes to your existing Management of Change (MOC) procedure rather than creating a parallel one.
- Attach section 6 (service provider requirements) and section 7 (product supplier requirements) to contracts and purchase specifications.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

How this document connects

Document or register	How records and decisions flow
OT-06 Standard 4.14 and 4.16	Technical detail for change and supplier controls
OT Workbook Exception Register	Legacy exceptions under section 8
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Integrator proposes a firmware update → MoC ticket with security impact check (section 5) → tested on spare controller → approved by Steering Committee → applied in shutdown → asset inventory updated.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Security Policy

[Company Name]'s commitment, objectives, values, risk appetite and accountabilities for the cybersecurity of its operational technology.

Organization	[Company Name]
Document ID	OT-04
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- This is the Tier 1 policy. Keep it short and strategic; technical requirements belong in the OT Security Standard (OT-06) and system-specific risks in the OT risk register (OT-05).
- Have your Board or Executive set the risk appetite in section 5.1 before publishing.
- Agree sections 2.2, 4 and 9 with Operations and Health & Safety. OT security only works when operations owns it too.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

How this document connects

Document or register	How records and decisions flow
OT-05 Risk Method	Rates risks against the appetite in 5.1
OT-06 Standard	Technical requirements under the policy
OT-03 Governance	Exceptions and escalation
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Policy statement 'no direct IT-to-OT traffic' → OT-06 4.9 conduit rules → firewall review finds an any-any rule → R-015 → fixed in next window.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Cyber Risk Management Methodology

A consequence-based method combining NIST SP 800-82r3 risk management with the ISA/IEC 62443-3-2 zone, conduit and security level process.

Organization	[Company Name]
Document ID	OT-05
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Rate risks with operations and Health & Safety in the room. Consequences are their expertise.
- Adjust the production and financial thresholds to your plants before first use.
- Record risks in the OT-Workbook Risk Register and zones in the Zones & Conduits sheet; the workbook flags safety consequences and SL gaps automatically.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

How this document connects

Document or register	How records and decisions flow
OT-04 Policy 5.1	Risk appetite and tolerable risk
OT-06 Standard	Countermeasures chosen in section 7
OT-08 Assessment Toolkit	Findings F-NNN feed new risks
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Assessment finding F-006 'engineering laptop shared with office use' → scenario risk R-017 (likelihood 3 × consequence 4) → SL-T 2 for the engineering zone → OT-06 4.6 hardening → residual risk Medium.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Security Standard

Technical security requirements for [Company Name]'s industrial control systems, organized by the ISA/IEC 62443 foundational requirements, with a system security requirements checklist for procurement.

Organization	[Company Name]
Document ID	OT-06
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- This is the Tier 3 technical standard under the OT Security Policy (OT-04). Use it with the OT Risk Management Methodology (OT-05), which sets the target security level of each zone.
- Replace every [bracketed] value with what your sites can actually achieve.
- Use Appendix B as the security requirements schedule in OT tenders and as the acceptance test checklist.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Jan 2008	A teenager used a modified TV remote control to switch tram points in a Central European city, derailing four trams and injuring about a dozen people. The signalling interface accepted commands with no authentication.	Unauthenticated commands to field equipment are a real risk (4.3, 4.9).

Summarized by CyberGlass from public reporting: US Senate testimony, Jun 2021; Company statements and public reporting, 2017; European press reporting, 2008. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
OT-04 Policy	Policy basis
OT-05 Risk Method	SL-T for each zone sets which requirements apply
OT-10 Shop Floor Checklist	Field verification of 4.6, 4.15 and 4.17
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Vulnerability advisory for an HMI (CVSS 9.8) → compensating control in 7 days (block port at conduit) → vendor-qualified patch in next shutdown → Vulnerabilities sheet closed.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Security Strategy and 24-Month Roadmap

Sets the direction, priorities, investment and phased roadmap for securing [Company Name]'s operational technology over the next 24 months.

Organization	[Company Name]
Document ID	OT-07
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Complete the OT Security Assessment (OT-08) first. The strategy should start from evidence, not assumptions.
- Keep it short enough for leadership to read in 15 minutes. Detail belongs in the roadmap table and the workbook.
- Agree the phase timings with operations so work fits planned maintenance windows and turnarounds.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Sep 2025	Ransomware at a third-party supplier of shared check-in and boarding software disrupted Heathrow, Brussels and Berlin airports, forcing manual check-in. The EU cybersecurity agency confirmed a 'third-party ransomware incident'.	Supplier-hosted systems are part of your OT risk.

Summarized by CyberGlass from public reporting: Public reporting summarized on Wikipedia, Oct 2025; ENISA Transport Threat Landscape, Mar 2023; ENISA statement reported by TechCrunch, Sep 2025. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
OT-08 Assessment	Current state (section 4)
OT-01 Charter	Objectives the roadmap delivers
OT Workbook KPIs	Section 8 measures
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: OT-08 maturity score 1.4 → roadmap target 2.5 in 24 months → Phase 1 funds jump host and backups → KPI 'priority zones monitored' moves 0% → 60%.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Security Assessment Toolkit

A practical method, question set, evidence checklist and maturity scoring model for assessing OT security at [Company Name] sites.

Organization	[Company Name]
Document ID	OT-08
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Use it for your first baseline and then yearly. Keep the same scoring so results can be compared over time.
- Agree the rules of engagement with operations before you start. The default is passive, read-only work.
- Score from evidence. If you cannot see it, score it as not in place and note what evidence is missing.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

Document or register	How records and decisions flow
OT-10 Checklist	Physical evidence
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Finding F-003 'flat network between office and control' → priority 1 (section 7) → risk R-001 → remediation plan item in next shutdown → re-assessed next year.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

CYBERGLASS OT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

OT Incident Response Playbooks

OT-specific response principles, roles and playbooks that extend the Incident Response Plan (IT-06) to industrial control systems at [Company Name].

Organization	[Company Name]
Document ID	OT-09
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Use this with the Incident Response Plan (IT-06). IT-06 sets the overall process; this document covers what is different in OT.
- Review each playbook with operations and your control system vendors. Add site-specific steps such as manual operating procedures.
- Exercise at least one playbook a year with the control room, not just the IT team.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

When	What happened	What it means for this document
Dec 2015	Attackers used stolen VPN credentials and remote control of operator HMIs to open breakers at three electricity distribution companies. About 225,000 customers lost power for several hours; field devices were deliberately bricked to slow recovery.	Loss of control from remote takeover (5.2, 5.5); manual operation must be practised.

Summarized by CyberGlass from public reporting: Public reporting summarized on Wikipedia, Oct 2025; Public ICS security reporting, 2017–2018; E-ISAC and SANS ICS analysis, 2016. Organizations are described, not named. Figures are as publicly reported at the time.

How this document connects

Document or register	How records and decisions flow
IT-06 Incident Response Plan	Overall process and notification
OT-04 Policy	Safety first value
OT Workbook (Risk Register, Asset Inventory, Remote Access, Zones & Conduits)	Live records: R-NNN, assets, remote paths, SL-T gaps
OT-09 Incident Response Playbooks / IT-06	Incidents INC-YYYY-NNN; root causes return to the risk register

Record flow example: Unexpected setpoint change on Line 2 (playbook 5.3) → INC-2026-041 → logic compared with offline backup → restored → root cause 'shared engineering account' → R-019 → OT-06 4.3 fix.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop