CYBERGLASS IT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Cybersecurity Program Charter

Establishes the cybersecurity program at [Company Name]: its mandate, scope, objectives, roles and authority.

Organization	[Company Name]
Document ID	IT-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.

- Complete this first. Every other document in the kit refers back to it.
- Get it signed by the most senior leader you can (owner, CEO or president). The signature is what gives the program authority.
- Set 3–5 objectives you can actually measure in 12 months. You can add more later.
- 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
Jul 2025	The global average cost of a breach was US$4.44M. 13% of organizations reported breaches of AI models or applications, and 97% of those said they lacked proper AI access controls.	Breach cost is a leadership issue; use it to justify the budget in section 9.

Summarized by CyberGlass from public reporting: US Senate testimony, Jun 2021; Verizon Data Breach Investigations Report 2025; IBM Cost of a Data Breach Report 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
IT-03 Governance Framework	Turns the charter's mandate into a committee, RACI, exception route and reporting calendar
IT-04 Information Security Policy	States the rules the charter authorizes; approved by the same Executive Sponsor
IT-05 Risk Method and workbook Risk Register	Objectives in section 4 trace to risks R-NNN they reduce
IT-02 First 90 Days Plan	Delivers the first objectives; the day-90 report updates section 10 measures
Workbook KPIs sheet	Calculates the section 10 measures every quarter

Record flow example: Objective 1 (MFA, Month 3) reduces risk R-003 'account takeover'; progress is reported from the KPIs sheet each quarter to the Steering Committee (IT-03).

PREVIEW

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

CYBERGLASS IT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

First 90 Days Plan

A practical 30-60-90 day plan for a new cybersecurity program manager or first security hire at [Company Name].

Organization	[Company Name]
Document ID	IT-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.

- Adjust dates to your start date. Keep the three phases: learn, fix the basics, set the program.
- Share this plan with your sponsor in week 1 so expectations are agreed.
- Tick off items as you go and attach the evidence; it becomes your 90-day report.
- 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

Record flow example: An interview reveals a shared admin password (day 12) → logged as R-007 → fixed as a quick win by day 45 → closed in the register with evidence.

PREVIEW

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

CYBERGLASS IT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Cybersecurity Governance Framework

How cybersecurity decisions are made, approved, reported and reviewed at [Company Name].

Organization	[Company Name]
Document ID	IT-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.

- Match the committee members to your real organization. In a small company the committee may be three people.
- Use the RACI in the workbook (IT-Workbook, RACI sheet) to adjust who does what.
- Keep the exception process strict: every exception needs an owner and an expiry date.
- 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

IT-01 Charter	Source of the committee's authority
IT-04 Policy	Exceptions to the policy follow section 5 and are logged as E-NNN
IT-05 Risk Method	Risk acceptance authority (section 6) uses the same rating bands
Workbook Exception Register and RACI sheets	Hold the live records for sections 5 and 8

Record flow example: A legacy server cannot run the new endpoint agent → exception E-004 raised under section 5 with compensating controls → accepted by the authority in section 6 → reviewed every 90 days until retired.

PREVIEW

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

CYBERGLASS IT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Information Security Policy

[Company Name]'s top-level policy for protecting information, systems and services, including the responsible use of artificial intelligence.

Organization	[Company Name]
Document ID	IT-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 top-level policy that leaders approve. Keep it short; put detail in the supporting standards listed in section 6.
- Replace every [bracketed] value with what your organization can actually achieve.
- Review section 7.6 (AI) with your privacy and legal advisers; AI rules are changing quickly.
- 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
Apr 2023	Engineers at a large electronics manufacturer pasted confidential source code and meeting notes into a public AI chatbot. The company then restricted generative AI tools on company devices.	Section 7.6 sets AI rules. Without them, staff paste confidential data into public tools.

Summarized by CyberGlass from public reporting: Company testimony and TechTarget, Apr–May 2024; Verizon Data Breach Investigations Report 2025; Public reporting, May 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
STD-01 Access Management and STD-02 Remote Access Standards	Detailed technical requirements under sections 7.3 and 7.7
IT-05 Risk Method	Section 7.1 risk management follows it
IT-06 Incident Response Plan	Section 7.11 reporting and response
IT-07 BC/DR Plan	Section 7.12 backup and continuity
AI-02 AI Acceptable Use Policy	Detailed rules behind section 7.6
Workbook Exception Register	Policy exceptions under section 8 (E-NNN)

Record flow example: A staff member reports a phishing email (7.5) → logged as INC-2026-014 (IT-06) → root cause 'MFA missing on one SaaS app' becomes risk R-021 → fixed and verified under 7.3.

PREVIEW

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

CYBERGLASS IT CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Cyber Risk Management Methodology

How [Company Name] identifies, rates, treats and reviews cybersecurity risks.

Organization	[Company Name]
Document ID	IT-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.

- Adjust the impact scale dollar amounts to the size of your business before first use.
- Record risks in the IT-Workbook (Risk Register sheet); it calculates scores and ratings automatically using these scales.
- Start with the 20 starter risks in the workbook (summarized in section 8) and keep only those that apply.
- 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
Jul 2025	The global average cost of a breach was US$4.44M. 13% of organizations reported breaches of AI models or applications, and 97% of those said they lacked proper AI access controls.	A reference point for financial impact bands; calibrate to your own revenue.

Summarized by CyberGlass from public reporting: Verizon Data Breach Investigations Report 2025; Public reporting summarized on Wikipedia, Oct 2025; IBM Cost of a Data Breach Report 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
Workbook Risk Register	Every risk rated with this method is recorded as R-NNN
IT-03 Governance Framework	Risk acceptance authority by rating
IT-06 Incident Response Plan	Each Severity 1–2 incident triggers a risk review
AI-03 AI Risk Method	Uses the same 5×5 scales so AI risks (AR-NNN) can be compared
CSF-03 Gap Analysis	Priority gaps become risks and treatment actions

Record flow example: Supplier review finds no MFA at a payroll provider → risk R-012 rated 3 × 4 = High (section 6) → owner accepts treatment 'contract clause and MFA by Month 4' → reviewed quarterly until closed. Shared IDs: INC-YYYY-NNN incidents (IT-06 Appendix B, OT-09, AI-05) · R-NNN risks (kit workbook) · AR-NNN AI risks · E-NNN exceptions · F-NNN assessment findings · SF-NNN shadow AI findings · TR-NNN AI tool requests · SC-NNN security conditions (rail) · A-NN action plan items.

PREVIEW

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

CYBERGLASS CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Incident Response Plan

How [Company Name] prepares for, detects, responds to and recovers from cybersecurity incidents and privacy breaches.

Organization	[Company Name]
Document ID	IT-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.

- Fill in the contacts first (Appendix C and the workbook Contacts sheet). In a real incident, the contact list is what people reach for.
- Agree section 5.1 and section 7 with your Executive Sponsor, insurer and legal counsel before an incident happens.
- Keep a printed copy offline: email and shared drives may be unavailable during an attack.
- Run a tabletop exercise within 90 days of approval and update the Plan with what you learn.
- 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
Jun 2017	Destructive malware spread through a compromised accounting-software update and wiped tens of thousands of devices at a global shipping company. It rebuilt its IT estate in about ten days; losses were reported at around US$300M.	Recovery (6.5) depends on clean backups and a known rebuild order; practise it.
Jan 2024	A finance employee in the Hong Kong office of a global engineering firm transferred about US$25M (HK$200M) after a video call in which the 'CFO' and other colleagues were all deepfakes.	Payment fraud by impersonation is an incident too; the payment-fraud playbook (section 10) must cover voice and video.
Jul 2024	A faulty content update from a security software vendor crashed about 8.5 million computers worldwide, stopping airlines, hospitals and banks. Many devices needed hands-on recovery one by one.	Not every incident is an attack. Severity and process must also work for a vendor-caused outage.

Summarized by CyberGlass from public reporting: Company testimony and TechTarget, Apr–May 2024; Company statements and public reporting, 2017; CNN and SCMP, May 2024; Vendor and platform statements, Jul 2024. 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-07 BC/DR Plan	Invoked from section 6.4–6.5 when recovery exceeds RTO
AI-05 AI Incident Playbook	AI-specific steps; same INC-YYYY-NNN log
OT-09 / RAIL kit playbooks	Safety-first steps when operations are affected
Workbook Risk Register	Root causes become or update risks R-NNN after 6.6
Workbook Contacts sheet	Live version of Appendix C

Record flow example: AI-06 review finds staff pasting customer data into a free chatbot (SF-003) → reported as INC-2026-031 (Severity 3) → AI-05 playbook 5.1 → root cause recorded as risk AR-007 and R-018 → AI-02 training refreshed.

PREVIEW

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

CYBERGLASS CYBERSECURITY PROGRAM · FOUNDATIONS KIT

Business Continuity and Disaster Recovery Plan

How [Company Name] keeps critical activities running during a disruption and recovers its systems and data within agreed times.

Organization	[Company Name]
Document ID	IT-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.

- Start with the business impact analysis in the BC/DR Workbook. Recovery priorities only make sense once process owners have rated their impacts.
- Agree RTO and RPO with process owners and leadership, then check that systems and suppliers can actually meet them (Systems sheet). Make sure every critical SaaS service has a copy of its data outside the provider.
- Keep printed or offline copies of this Plan and the contact lists: shared drives may be unavailable during a disruption.
- Exercise the Plan within 90 days of approval and record the results in the Test Log sheet.
- 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

Real-world context: why this document matters

When	What happened	What it means for this document
Sep 2025	A cyberattack forced a UK carmaker to halt global vehicle production from 1 September 2025; a phased restart began only in October. Hundreds of suppliers were hit, and the wider UK economic cost was estimated at about £1.9 billion.	Production stopped for weeks. The BIA (section 6) must show maximum tolerable downtime for each critical process, not just IT systems.
Jul 2024	A faulty content update from a security software vendor crashed about 8.5 million computers worldwide, stopping airlines, hospitals and banks. Many devices needed hands-on recovery one by one.	Recovery strategies (section 8) must cover mass endpoint failure, not only server loss.
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'.	When a supplier platform fails, manual workarounds (section 10.2) keep the business running; write and rehearse them.

Summarized by CyberGlass from public reporting: Public reporting summarized on Wikipedia, Oct 2025; Vendor and platform statements, Jul 2024; 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
IT-06 Incident Response Plan	Cyber incidents escalate here when recovery exceeds RTO
BCDR Workbook (BIA and Recovery)	Holds BIA results, recovery tiers, test log
Workbook Asset Inventory	Systems and dependencies feeding the recovery order
Workbook Risk Register	Recovery gaps (RTO not achievable) are recorded as risks

Record flow example: BIA sets payroll RTO 48 h → DR test restores payroll in 70 h → gap recorded as R-024 → fix funded → retest passes → Test Log updated.

PREVIEW

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