



Information security policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-IS	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

Example Machining Ltd. ("Example Machining") protects the information it holds for its clients, its customers, its staff, and itself. This policy sets management's direction for information security, names who is responsible, and lists the policies that support it.

2. Scope

This policy applies to all employees, contractors, term staff, and service providers who use Example Machining systems, devices, facilities, or information, wherever they work.

3. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

4. Management commitments

Example Machining management commits to protecting the confidentiality, integrity, and availability of the information it is responsible for, meeting the security requirements in its contracts and in applicable law, providing the people, time, and tools needed to follow these policies, and correcting its controls when a review, an incident, or a change shows a gap.

Where a Government of Canada defense contract requires it, Example Machining completes the Canadian Program for Cyber Security Certification (CPCSC) Level 1 self-assessment every year, records the result and its expiry date in the company's CanadaBuys supplier profile, and keeps the supporting evidence for at least one year.

Personal information is handled in line with the Personal Information Protection and Electronic Documents Act (PIPEDA) and any other Canadian privacy law that applies to Example Machining.

5. Roles and responsibilities

The President approves this policy set and provides the resources to carry it out. The IT Manager maintains the policies, keeps the registers and logs they call for, runs the scheduled reviews, and reports on security to the President. Managers see that their teams follow these policies and report access

changes promptly. Every person covered by this policy follows it and reports suspected security incidents.

6. Awareness and training

Everyone covered by this policy reads the policy set when they start and confirms in writing that they have read it. Security awareness training is given at onboarding and at least once a year after that, and attendance is recorded.

7. Reporting security events

Suspected security incidents, lost or stolen devices, phishing messages, and policy breaches are reported to security@example.ca without delay. Reporting something in good faith never leads to discipline, even if it turns out to be a false alarm.

8. Supporting policies

The following policies form part of the Example Machining information security policy set:

POLICY	ID	VERSION
Access control and account management policy	POL-AC	1.0.0
Approved systems and external systems policy	POL-ES	1.0.0
Public information policy	POL-PI	1.0.0
Identification and authentication policy	POL-IA	1.0.0
Media sanitization and disposal policy	POL-MP	1.0.0
Physical security policy	POL-PE	1.0.0
Network boundary protection policy	POL-SC	1.0.0
Patch and flaw remediation policy	POL-FR	1.0.0
Malicious code protection policy	POL-MC	1.0.0
Incident response policy	POL-IR	1.0.0
Change management policy	POL-CM	1.0.0
Backup and recovery policy	POL-BR	1.0.0

9. Records kept

These records are kept as evidence that the policy is followed:

- Signed and dated copy of this policy
- Staff acknowledgement records
- Security awareness training attendance records

- CPCSC Level 1 self-assessment result and CanadaBuys profile record

10. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

11. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

12. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library @ 2026 Hans Study, CC BY 4.0`



Access control and account management policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-AC	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy sets how Example Machining creates, approves, reviews, and removes user accounts, and how access to SI is limited to the people whose work needs it.

2. Scope

It covers every account on Example Machining systems, including cloud services, network equipment, shop-floor terminals, and shared devices, and every employee, contractor, and service provider who holds one.

3. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

SI system. Any system, cloud service, or device that stores, processes, or sends SI.

Privileged account. An account that can change system settings, security controls, or other users' access.

4. Account types

These account types are allowed: individual user accounts assigned to one named person; separate administrator accounts for staff who manage systems, used only for administrative work; and service accounts that run software, each with a named owner.

Shared, generic, and guest accounts are prohibited on SI systems and on administrative interfaces. Vendor default accounts are disabled, or renamed and given a new password, before a system goes into use.

5. Requesting and approving access

Accounts are created, enabled, changed, disabled, and removed only through a written request approved by the person's manager and carried out by the IT Manager or a delegate. A ticket or an email is enough, as long as it records who needs access, to which systems, and why.

Access is granted only when an approved request exists and only to the systems the person needs for their role. Access to SI is limited further, to the people working on the contract or project it belongs to.

The IT Manager keeps an account register for every system that holds SI. For each account it records the user's name, role, and employment status, the systems accessed, group and role memberships, privileges, and the dates the account was created, last changed, and disabled.

Contractor, term, and temporary accounts carry an expiry date no later than the end of the engagement. Extending one takes a new approved request.

6. Least privilege

Permissions are assigned to role-based groups such as finance, projects, production, HR, and IT, and people are added to the groups they need; permissions are not granted to individuals directly except under an approved exception. Systems are configured so that these approved permissions are enforced for SI and for system settings and resources.

Everyday user accounts do not have local administrator rights on laptops or desktops. Staff who need software installed request it through the IT Manager.

7. Monitoring account use

The IT Manager reviews sign-in activity on SI systems monthly, looking for sign-ins at unusual hours or from unexpected locations, repeated failures, and any activity on accounts that should be disabled.

8. Disabling and removing accounts

An account is disabled when any of the following applies:

- it reaches its expiry date
- it has not been used for 45 days
- it is no longer tied to a current employee, contractor, or owner
- it has been used in breach of a Example Machining policy
- the President or the IT Manager identifies a significant risk tied to the account holder

The Office Manager tells the IT Manager by the end of the same business day after someone leaves or transfers to another role, and the account is disabled as part of offboarding. Managers tell the IT Manager within 5 business days when a person's duties change enough to affect their access or need-to-know, and when an account is no longer required.

Accounts of staff on leave longer than 30 days are disabled for the length of the leave and enabled again on their return.

9. Logging out

Users log out of SI systems at the end of each workday, when leaving a shared workstation, and after 8 hours without use.

10. Access reviews

The IT Manager reviews all accounts, group memberships, and shared folder permissions quarterly, with each manager confirming their team's access. Each review is recorded with the date, the reviewer, and the changes made.

11. Records kept

These records are kept as evidence that the policy is followed:

- Account register
- Approved access requests
- Access review records
- Sign-in review notes
- List of disabled accounts with dates
- Departure and transfer notices from HR

12. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

13. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

14. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study` · Generated at `hans.study/tools/policy-builder` · Clause library © 2026 Hans Study, CC BY 4.0

S

Approved systems and external systems policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-ES	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy sets which systems, cloud services, and devices may be used for Example Machining work, and when a system the company does not own or manage may be used at all.

2. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

SI system. Any system, cloud service, or device that stores, processes, or sends SI.

External system. A system that Example Machining does not own or manage, including personal devices, home networks, public computers, and personal email or cloud accounts.

3. Approved systems list

The IT Manager maintains an approved systems list naming every system, cloud service, application, and device type approved for Example Machining work, and marks which of them are approved for SI. The list is kept in the IT folder on the shared drive, where every staff member can read it.

New staff are shown the approved systems list during onboarding and told which tools they may not use for work.

Staff who want a new application, browser extension, or online service for work request it through the IT Manager. Nothing is installed, and no account is opened with a company email address, until the request is reviewed and the tool is added to the list.

Before a new cloud service is added to the list, the IT Manager records where the provider stores data, which countries' laws can compel the provider to hand it over, whether it supports multi-factor authentication and encryption, and how data is returned or deleted when the service ends.

4. External systems

Staff must not use an external system to reach Example Machining systems or to process, store, or send SI unless it is on the approved systems list or covered by a written authorization. This includes personal email and cloud storage accounts, personal computers and phones, home or public computers, and AI tools or file converters that are not on the list.

Before an external system is authorized, it must meet these requirements:

- an operating system that still receives security updates, with updates applied
- full-disk encryption turned on
- anti-malware protection running and up to date
- an automatic screen lock
- multi-factor authentication on any account used to reach Example Machining systems

An external system is used only after the IT Manager has checked that it meets these requirements and a signed agreement is on file. For a personal device, the agreement is the user's signed acknowledgement of this policy and of Example Machining's right to remove company data from the device. For a partner or service provider's system, it is a contract or connection agreement that states the security requirements.

Example Machining USB drives, external disks, and memory cards must not be connected to external systems.

5. Records kept

These records are kept as evidence that the policy is followed:

- Approved systems list
- Signed personal device acknowledgements
- Partner and service provider agreements with security terms
- Cloud service review records
- Onboarding training records

6. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

7. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

8. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0

S

Public information policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-PI	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy keeps SI off Example Machining's website, social media, and other public channels, and sets out what to do if any gets through.

2. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

Controlled area. A room, area, or cabinet where SI is stored, processed, or printed, or where equipment that holds it is located.

3. Authorized publishers

Only people named on the authorized publisher list may post to the Example Machining website, social media accounts, news releases, sales and trade show material, and bulk email. The President approves the list.

Before being added to the list, each publisher is trained to recognize SI and what must stay out of public content, and repeats the training every year. Training records are kept.

For government work, content that must stay private includes contract numbers, drawings, specifications, part numbers, delivery schedules, and photographs of work in progress.

4. Review before release

Every item is checked by someone other than its author before release, using this checklist:

- Does it contain SI or details from a client contract?
- Does it name a government program, client, or site without written permission?
- Does a photo or video show drawings, screens, whiteboards, parts, or restricted areas?
- Does it reveal network details, system names, or staff email formats useful to an attacker?

Any "yes" stops the item until the content is removed or the owner of the information approves it in writing.

5. Review after release

The Communications Lead rechecks content already on public systems quarterly, including older website pages, uploaded documents, and the metadata in published images and PDFs.

If SI is found on a public system, it is taken down at once, security@example.ca is notified, and the event is recorded as a security incident. Any client or contracting authority is notified as its contract requires.

6. Records kept

These records are kept as evidence that the policy is followed:

- Authorized publisher list
- Publisher training records
- Completed pre-release checklists
- Public content review records
- Incident records for removed content

7. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

8. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

9. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`



Identification and authentication policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-IA	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy sets how people and devices prove who they are before they reach Example Machining systems.

2. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

SI system. Any system, cloud service, or device that stores, processes, or sends SI.

Privileged account. An account that can change system settings, security controls, or other users' access.

3. User identification

Every user has a unique user ID. Credentials are never shared, including with IT staff, managers, or vendors.

Every user is authenticated before reaching any Example Machining system. Accounts without a password or other authenticator are not permitted.

Scripts, scheduled tasks, and integrations run under registered service accounts with a named owner, so every automated action traces back to a responsible person.

4. Passwords and screen locks

Passwords are at least 14 characters, and passphrases made of several unrelated words are encouraged. A work password is never reused on any other account or website. Passwords are changed when compromise is suspected, not on a fixed calendar, and systems that can check new passwords against lists of known breached passwords do so.

Laptops and desktops lock after 15 minutes without use, and phones and tablets after 5 minutes. Users lock their screen whenever they step away.

Users must sign in again in these situations:

- after a screen lock or session timeout

- before using administrator rights
- before changing their password or multi-factor settings
- when signing in from a new device or location

5. Multi-factor authentication

Multi-factor authentication (MFA) is required on every account on SI systems, every privileged account, and all remote access. The requirement covers privileged and non-privileged accounts alike.

MFA uses an authenticator app with number matching, or push approvals that show where the sign-in is coming from. Text-message codes are allowed only as a temporary fallback approved by the IT Manager.

A user who loses an MFA device reports it to the IT Manager the same day. Before a new factor is issued, the IT Manager confirms the user's identity in person or on a video call with photo ID; an email, text, or voicemail request is never enough on its own.

6. Device identification

Only these device types may connect to Example Machining systems: laptops, desktops, servers, phones, tablets, printers, and network equipment. Each device is listed in the device inventory with its asset number, serial number, type, model, assigned user, and approval date.

Devices are authenticated before reaching company systems through device management enrolment and conditional access rules that allow sign-in only from enrolled, compliant devices. On the office network, company devices join Wi-Fi through WPA2-Enterprise or WPA3-Enterprise using a device credential, and unused wired ports are disabled. A shared Wi-Fi passphrase on its own does not count as device authentication.

USB storage devices not issued by Example Machining are blocked on company computers through device control settings.

Visitors and personal devices use a guest Wi-Fi network separated from internal systems, with internet access only. Its password changes at least every quarter.

7. Records kept

These records are kept as evidence that the policy is followed:

- Account list showing unique user IDs
- MFA configuration screenshots and enrolment reports
- Password and screen lock configuration settings
- Device inventory
- Conditional access or 802.1X policy export
- MFA reset records with identity checks

8. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

9. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

10. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`

S

Media sanitization and disposal policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-MP	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy makes sure no SI can be recovered from media once it leaves Example Machining's control or is handed to someone else.

2. Scope

It covers all media that has held SI or other Example Machining data, whether owned, leased, or on loan.

3. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

Media. Anything that stores data, including hard drives, solid-state drives, USB drives, memory cards, phones, tablets, and the internal storage in printers, copiers, and network equipment.

4. When media is sanitized

Media is sanitized before any of the following:

- disposal or recycling
- return to a leasing company or vendor
- shipping out for repair or warranty service
- sale or donation
- reuse by another person, or for another purpose, inside Example Machining

5. Sanitization methods

Staff sanitize media following the Canadian Centre for Cyber Security's IT media sanitization guidance (ITSP.40.006) or NIST SP 800-88. Hard disk drives are overwritten with a wipe tool that produces a verification report. Solid-state drives, phones, and tablets are sanitized with cryptographic erase or the manufacturer's secure erase command, because overwriting does not reach every storage cell on flash media. Each wipe is verified before the media leaves Example Machining's control.

Media that cannot be sanitized and verified, is damaged, or held SI and has little resale value is physically destroyed by shredding, crushing, or disintegration. It is not sold, donated, or given to staff.

Before a leased printer, copier, or multifunction device goes back, its internal storage is removed and destroyed, or the lessor provides a sanitization certificate naming the device's serial number.

Where possible, storage is removed from a device before it ships for warranty repair. If the drive cannot come out, the device is sanitized before it ships or the repair is done on site.

6. Disposal records

Every item is recorded in the disposal log with its asset number, serial number, media type, the method used, who did the work, the date, where the item went, and any certificate reference.

7. Records kept

These records are kept as evidence that the policy is followed:

- Disposal log
- Wipe tool verification reports
- Certificates of destruction
- Lease return sanitization certificates

8. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

9. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

10. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

S

Physical security policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-PE	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy controls who can physically reach SI and the equipment that holds it.

2. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

Controlled area. A room, area, or cabinet where SI is stored, processed, or printed, or where equipment that holds it is located.

3. Controlled areas

These areas are controlled areas: the server or network room, the engineering office, and any room or cabinet where SI is stored or printed. A floor plan marking them is kept with this policy.

4. Physical access list

The IT Manager maintains a physical access list naming everyone authorized to enter each controlled area, with the credential type (key, card, fob, or code), the date issued, and any expiry date. The President approves the list and each addition to it.

Keys, cards, fobs, and codes are issued only to people on the approved list, and each issue is recorded.

The list is reviewed quarterly against current staff and contractor records, and each review is recorded.

People come off the list on their last day, or as soon as their role stops needing access. Their keys, cards, and fobs are collected, their cards are deactivated the same day, and any shared door codes or combinations they knew are changed.

Access for contractors, term staff, and other temporary people expires after at most 90 days or at the end of their engagement, whichever comes first.

5. Entry control

Entry to controlled areas is managed by an electronic access control system that checks each credential against the approved list before it releases the door. Exit-only doors are alarmed so they cannot be used to enter. Controlled area doors stay closed and locked, with door-held-open alarms turned on.

Staff do not hold controlled area doors for anyone they cannot confirm is authorized. Signs at those doors remind staff of this rule.

Access control system event logs are kept for at least 1 year.

6. Visitors

Visitors sign in with their name, organization, host, and times in and out, show photo ID, and wear a visitor badge. Inside controlled areas their host escorts them at all times, and they are never left alone with SI, open computer sessions, or network equipment. The visitor log is kept for at least 1 year.

7. Keys, cards, and combinations

Spare keys, master keys, and unissued cards are kept in a locked key cabinet with a sign-out log. Combinations and keypad codes are changed at least once a year, when anyone who knows them leaves, and after any suspected compromise, and every change is recorded.

8. Printers and printed information

Printers that may print SI use secure print release, holding each job until the user authenticates at the printer.

Printed SI is kept in locked cabinets or a locked room when not in use. It is not left on desks, printer trays, or meeting tables.

9. Records kept

These records are kept as evidence that the policy is followed:

- Floor plan marking controlled areas
- Physical access list and review records
- Credential issue and return records
- Access control event logs or area sign-in sheets
- Visitor logs
- Key cabinet sign-out log and combination change records
- Secure print configuration or printer location records

10. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

11. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

12. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`

S

Network boundary protection policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-SC	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy controls what traffic can cross into, out of, and within the Example Machining network.

2. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

SI system. Any system, cloud service, or device that stores, processes, or sends SI.

Managed interface. A firewall or other boundary device under Example Machining's control that network traffic must pass through.

3. Internet boundary

Every internet connection passes through a business-grade firewall managed by Example Machining or its managed service provider. An internet provider's modem or a consumer router is never the security boundary; where the provider's equipment cannot be removed, it is set to bridge mode upstream of the firewall.

The firewall blocks all inbound traffic by default. Each inbound rule is documented with its purpose, owner, and the date it was added. No management interface, whether for a firewall, switch, camera recorder, or server console, is reachable from the internet.

Outbound traffic is limited to what the business uses. At a minimum, outbound file sharing (SMB) is blocked and known malicious destinations are filtered through DNS or web filtering.

External connections are made only through the managed firewall. Cellular hotspots, secondary internet connections, and unmanaged wireless bridges are not connected to internal networks, and remote-control tools that tunnel around the firewall are used only if listed on the approved systems list.

4. Monitoring

Firewall logs, including traffic between internal segments, are sent off the firewall to a log server or cloud service, kept for at least 1 year, and reviewed quarterly. Alerts are set for configuration changes and for repeated blocked attempts against management services.

5. Internal segmentation

The internal network is divided into segments with firewall rules between them. At a minimum, these are kept apart:

- staff computers
- servers and SI systems
- guest Wi-Fi
- production and shop-floor equipment such as CNC machines and PLCs
- cameras, access control, and other building systems

Traffic between segments is allowed only by documented rules.

Systems the public can reach, such as a website, customer portal, or file transfer service, sit in a separate subnetwork (DMZ) or are hosted outside the internal network entirely. They cannot open connections into internal segments.

6. Remote access

Remote access to internal systems uses the company VPN with multi-factor authentication. The VPN portal is kept on current firmware and is included in the firewall rule review.

7. Documentation and change control

The IT Manager keeps a current network diagram showing internet connections, firewalls, segments, and public-facing systems. Every firewall and network change goes in a change log with the date, the reason, and who made it.

Firewall rules are reviewed quarterly, and rules that are unused or have no owner are removed.

8. Records kept

These records are kept as evidence that the policy is followed:

- Network diagram
- Firewall configuration export or screenshots
- Firewall rule review records
- Network change log
- Log forwarding and retention settings
- Remote access configuration

9. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

10. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

11. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`



Patch and flaw remediation policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-FR	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy sets how Example Machining finds and fixes security flaws in its systems, and how quickly updates go in.

2. Scope

It covers operating systems, browsers, applications, and firmware on every computer, server, phone, tablet, firewall, switch, wireless access point, and printer, plus connected building equipment such as camera recorders and access control panels.

3. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

SI system. Any system, cloud service, or device that stores, processes, or sends SI.

4. Finding and reporting flaws

The IT Manager checks these sources weekly and treats a flaw as identified on the day it appears in one of them:

- vendor security advisories for every product on the approved systems list
- Canadian Centre for Cyber Security alerts and advisories
- the CISA Known Exploited Vulnerabilities catalogue
- patch compliance reports from device management

Staff report failed updates, unsupported software, and suspected flaws to the IT Manager within one business day of noticing them. Each flaw is recorded with the date found, the affected systems, and its severity.

5. Fixing flaws

Flaws are corrected by installing the update, changing the configuration, or removing the affected software. Where no fix exists yet, the IT Manager records the interim measure, such as turning off the affected feature or isolating the device, until one is released.

Automatic updates are turned on for operating systems, browsers, and applications wherever the software supports them.

Updates for flaws that are being actively exploited, or that the vendor rates critical, are installed within 14 days of the vendor's release, and all other security updates within 30 days.

Security firmware updates for network equipment, servers, printers, and connected building devices are installed within 30 days of release. Equipment that can only be updated during a shutdown is scheduled into the next planned maintenance window, and if that falls outside the deadline the delay is logged as an exception.

Software and devices that no longer receive security updates are replaced. Until then they are isolated on a separate network segment and recorded as exceptions. This includes machine controllers and test equipment running old versions of Windows.

6. Records

A patch log records updates to servers, firewalls, and SI systems, with the date, the update, and who installed it. For laptops and phones, device management compliance reports are the record.

7. Records kept

These records are kept as evidence that the policy is followed:

- Advisory subscriptions
- Flaw tracking records
- Patch log
- Device management compliance reports
- Vulnerability scan reports
- Exception register entries for unsupported systems

8. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

9. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

10. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`

S

Malicious code protection policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-MC	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy keeps malicious code out of Example Machining systems and sets how detections are handled.

2. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

3. Where protection runs

Microsoft Defender Antivirus, or another product on the approved systems list, runs on every laptop, desktop, and server, and on phones and tablets where the platform supports it.

Email is filtered for malicious attachments and links before delivery. Web traffic is filtered against known malicious sites at the firewall or through a DNS filtering service.

4. Updates and scanning

Engines and definitions update automatically as new releases come out, and the IT Manager checks the management console monthly for devices that have stopped updating.

Real-time protection scans files as they are downloaded, opened, or run, including files on USB drives and in email attachments.

A full scan of each device runs weekly.

5. Responding to detections

Detected malicious code is blocked or quarantined automatically. Tamper protection is on, so users cannot turn off protection or add exclusions.

Detections alert the IT Manager, who investigates each one, confirms the device is clean, and records what was found, the action taken, and how it was resolved.

Exclusions are added only by the IT Manager, for a documented business reason, limited to the specific file or folder, and reviewed at every policy review.

Anyone who sees a malware warning, a ransom note, or files changing unexpectedly disconnects the device from the network by unplugging the cable or turning off Wi-Fi, leaves it powered on, and contacts security@example.ca right away. They do not try to clean the device themselves.

6. Records kept

These records are kept as evidence that the policy is followed:

- Console screenshots showing protection status on all devices
- Scan schedule and tamper protection settings
- Email and web filtering configuration
- Detection and resolution records
- Exclusion list with reasons

7. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

8. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

9. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0

S

Incident response policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-IR	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy sets how Example Machining detects, reports, contains, and recovers from security incidents, and who decides what along the way.

2. Scope

It covers any suspected or confirmed event that affects the confidentiality, integrity, or availability of Example Machining information or systems, including:

- malware or ransomware on any device
- a phishing message that captured a password or led to a payment
- a lost or stolen laptop, phone, USB drive, or backup disk
- access to a system or account by someone not authorized to use it
- SI sent, posted, or stored somewhere it should not be
- a break-in or unexplained entry to a controlled area
- a breach at a service provider that holds Example Machining data

3. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

4. Roles

The IT Manager leads the response and keeps the incident log. The President makes the business decisions, including shutting down systems or production, bringing in the company's managed service provider or incident response firm, and notifying clients, insurers, or authorities. If the IT Manager is unavailable or involved in the incident, the President names someone else to lead.

5. Incident response plan

The IT Manager keeps a written incident response plan with a contact list covering staff, the internet provider, the company's managed service provider or incident response firm, the cyber insurer, legal counsel, the bank, and police. A printed copy is kept in a locked location on site and another off site,

because the plan has to be readable when the network is down.

Each incident moves through these stages, and the incident log records the date and time each one starts:

- report and record the event
- contain it so it stops spreading
- remove the cause
- restore systems and data from known-good sources
- review what happened and what to change

6. Handling an incident

Staff report suspected incidents to security@example.ca straight away and do not wait to be sure. Every report goes in the incident log with the date and time, who reported it, what they saw, and the systems involved.

An affected device is disconnected from the network but left powered on, because shutting it down erases evidence held in memory. Passwords for affected accounts are reset from a device known to be clean, and active sign-in sessions for those accounts are revoked.

Logs, suspicious emails, and affected devices are kept unchanged until the IT Manager decides they are no longer needed. Nothing is wiped or rebuilt before copies are taken. Anyone who handles evidence records what they took, when, and where it is stored.

Example Machining does not pay a ransom or extortion demand without the approval of the President, advice from legal counsel and the cyber insurer, and a check that the payment does not break sanctions law.

The cyber insurer is notified within the notice period in the insurance policy. Outside firms are engaged through the insurer's approved list where the policy requires it, since using a firm outside that list can limit coverage.

7. Reporting outside the company

Where an incident affects SI, Example Machining notifies the contracting authority as its contracts require. The incident may also be reported to the Canadian Centre for Cyber Security.

When a breach of security safeguards involving personal information creates a real risk of significant harm, Example Machining reports it to the Office of the Privacy Commissioner of Canada and notifies the affected individuals as soon as feasible. A record of every breach involving personal information is kept for at least 24 months, whether or not it was reported.

8. After an incident

Within 15 days of closing a significant incident, the IT Manager holds a review covering what happened, how it was found, how long each stage took, and what will change. Changes to systems, policies, or training are assigned an owner and a date.

9. Testing and training

The plan is tested once a year with a tabletop exercise built around a realistic scenario, such as ransomware on the file server or a stolen laptop holding SI. The exercise is recorded, and gaps it finds go into the plan.

Staff learn how to recognize and report an incident as part of onboarding and the yearly awareness training. Anyone with a role in the plan also learns that role.

10. Records kept

These records are kept as evidence that the policy is followed:

- Incident response plan and contact list
- Incident log
- Post-incident review records
- Tabletop exercise records
- Breach records involving personal information
- External notifications sent

11. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

12. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

13. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`

S

Change management policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-CM	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy makes sure changes to Example Machining systems are planned, checked for their effect on security, and recorded, so that an outage or a weakened control can be traced to the change that caused it.

2. Scope

It covers changes to servers, firewalls, switches, wireless equipment, cloud service settings, security tools, SI systems, and production equipment such as machine controllers. Automatic updates handled under the patch policy and everyday changes to user files are outside its scope.

3. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

SI system. Any system, cloud service, or device that stores, processes, or sends SI.

4. Baseline configurations

The IT Manager keeps a documented baseline configuration for each SI system and network device, recording the operating system or firmware version, installed software, and security settings. The baseline is updated after every change, and a copy of each network device configuration is saved with it.

Running configurations are compared to the baseline quarterly. A difference with no matching change record is treated as a security incident until it is explained.

5. Types of change

Every change falls into one of these types:

- standard changes are low-risk and repeatable, such as adding a user through an approved access request, and are pre-approved once in writing
- normal changes need assessment and approval before they are made
- emergency changes are made to stop an incident or outage in progress, approved verbally, and documented afterward

6. Requesting and approving a change

A normal change request records what will change and why, the systems affected, the security impact, how it will be tested, how it will be rolled back, who will do it, and when.

Before approval, the effect on security controls is assessed. Changes that open firewall ports, add remote access, exempt an account from multi-factor authentication, or turn off logging or anti-malware need the reason written into the request.

The IT Manager approves normal changes. Changes that affect production, security controls, or SI systems also need the President's approval. Where only one person can both make and approve a change, the President signs off instead.

7. Making the change

The current configuration is backed up before any change to a network device or server. Changes are tested on a non-production system first where one exists.

Planned changes are made after 6 p.m. on weekdays or on weekends. Changes to production equipment are scheduled with operations so that a failed change does not stop a running job.

After a change, the person who made it confirms the system works, the security controls it touches are still in place, and the baseline is updated.

Emergency changes are written up and reviewed by the IT Manager within 2 business days.

8. Records

Every change goes in the change log with the date, requester, approver, description, result, and whether a rollback was needed.

9. Records kept

These records are kept as evidence that the policy is followed:

- Baseline configurations and saved device configurations
- Change requests and approvals
- Change log
- Emergency change reviews
- Baseline comparison records

10. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

11. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

12. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`



Backup and recovery policy

Example Machining Ltd.

POLICY ID	VERSION	EFFECTIVE	OWNER	APPROVED BY	REVIEW
POL-BR	1.0.0	2026-10-05	IT Manager	President	annually

1. Purpose

This policy makes sure Example Machining can recover its data and systems after hardware failure, ransomware, deletion, or a site outage.

2. What is backed up

The following are backed up:

- file servers and shared drives
- Microsoft 365 or Google Workspace mail, files, and sites
- accounting and ERP databases
- engineering files, including CAD models and CNC programs
- firewall, switch, and wireless controller configurations
- servers and virtual machines

Cloud services are backed up separately. Version history and recycle bins in Microsoft 365 or Google Workspace have time limits and can be emptied by an attacker who controls an administrator account, so they are not treated as backups.

3. Definitions

Specified Information (SI). Sensitive, unclassified Government of Canada information that a contract identifies as needing protection while a supplier handles it. It can include contract details not meant for public release, controlled goods information, and Protected information.

Media. Anything that stores data, including hard drives, solid-state drives, USB drives, memory cards, phones, tablets, and the internal storage in printers, copiers, and network equipment.

4. Copies and protection

At least 3 copies of backed-up data exist on at least 2 types of storage. One copy is held in cloud storage with immutability turned on, so it cannot be changed or deleted before its retention period ends, even by an administrator.

Backups run daily and are kept for 90 days.

Backups are encrypted in transit and at rest. Encryption keys and passphrases are kept apart from the backups themselves, in the password manager and in a sealed printed copy stored with the incident response plan.

The backup system uses its own administrator accounts with multi-factor authentication. Those accounts are not part of the main company directory, so a compromised domain or Microsoft 365 administrator cannot reach the backups.

Backups containing SI are stored only in locations and services that Example Machining's contracts allow for SI, and receive the same protection as the original data.

5. Monitoring

Failed or partial backup jobs alert the IT Manager, and each failure is fixed by the end of the next business day. The IT Manager also reviews job reports weekly for jobs that report success while backing up nothing.

6. Restore testing and recovery

Restores are tested quarterly by recovering a sample of files from each backup set to a separate location. At least once a year a full server or system is restored. Each test records what was restored, how long it took, and whether anything was missing.

The IT Manager keeps a recovery order listing which systems are restored first and how long the business can run without each one. The President approves the order.

Backup disks and tapes that are retired or fail are sanitized or destroyed under the media sanitization and disposal policy.

7. Records kept

These records are kept as evidence that the policy is followed:

- Backup job reports
- Restore test records
- Recovery order list
- Backup system configuration showing encryption and immutability

8. Exceptions

Exceptions to this policy require a written request to the IT Manager stating the business reason, the risk, the compensating measures, and an end date. The President approves or rejects each request. Approved exceptions go in the exception register and are reviewed at every policy review; none are open-ended.

9. Compliance

Breaching this policy may lead to loss of system access and disciplinary action, up to and including termination of employment or contract. Where a breach exposes SI, Example Machining notifies the contracting authority as its contracts require.

10. Review

The IT Manager reviews this policy annually, after any significant security incident, and when contract or legal requirements change. Changes take effect once the President approves them and staff have been told.

The review is completed before each annual CPCSC Level 1 self-assessment so that the policy matches what the assessment reports.

Prepared with the free policy builder at hans.study. Example Machining Ltd. may use, change, and share this document without restriction. It is a template, not legal advice, and it does not replace the security terms in the organization's own contracts.

`hans.study · Generated at hans.study/tools/policy-builder · Clause library © 2026 Hans Study, CC BY 4.0`