Information Security Policy

Template setup

Follow these setup instructions before publishing your policy:

1. *Insert "[Your Business Name]"*
2. *Insert "[Your Business Description]"*
3. *Insert your IT Contact's details*
    a. *Insert "[First name and Surname]"*
    b. *Insert "[Company name]"*
    c. *Insert "[Contact email]"*
    d. *Insert "[Contact number]"*
4. *(Optional) Under 3.2, set which information classification label you will use (currently "CONFIDENTIAL")*
5. *(Optional) Insert any additional policies from the* ***Suggested additional policies*** *at the bottom of this template*
6. *Once updated, review the policy for consistency and continuity with how your business operates and make any adjustments to align this policy with your existing security operations or activities (i.e. Add, remove, or adjust any policies)*
7. *Set the "Last reviewed:" date near the top of the policy*
8. *Remove these* ***Template setup*** *instructions and* ***Suggested additional policies*** *from this document.*

This template was created by DAOS Consulting.

DAOS
Business transformation &
Fractional CxO services

To contact us, go to www.daosconsulting.com

This is the Information Security Policy for [Your Business Name] – [Your Business Description]

This policy is for security fundamentals, and aims to align with the Australian ASD Essential Eight and New Zealand MBIE Protecting Business Data Guide

Last reviewed: April 01, 2025

---

1. Purpose and Scope

We operate as a small consulting team, and our priority is to safeguard our information, systems, with an emphasis on safeguarding client data and upholding an information security maturity that enables us to work with clients with essential cybersecurity needs. This policy outlines how we achieve that, whether we're working from our offices, home offices, or client workplaces. It applies to all employees, subcontractors, and third parties who access or manage our business assets.

---

2. Governance and responsibilities

- **Our leaders**: We ensure this policy is implemented by providing resources and oversight, reviewing it annually to maintain its effectiveness.
- **Our team**: We adhere to these guidelines and report any security incidents to our IT Contact within 24 hours.

- **Our IT Contact**: We make sure an IT Contact is available to manage technical security measures, including system configurations and periodic assessments, to keep our activities secure:
    - **IT Contact name**: [First name and Surname]
    - **IT Contact company**: [Company name]
    - **IT Contact email**: [Contact email]
    - **IT Contact phone/mobile**: [Contact number]
- We commit to adjusting practices to meet client needs and changes to minimum security recommendations.

---

3. Risk Management Controls

3.1 Asset Management

- We maintain an inventory of all business-owned devices (e.g. laptops, mobile phones), media (e.g. external hard drives), and software (including cloud software), assigning ownership to ensure accountability for their security and upkeep. The inventory keeps a note of:
    - The asset name
    - The asset model
    - The asset type
    - The status of the asset as active, not in use, or decommissioned
    - The maximum sensitivity of information stored
    - The authentication used
    - Any special security considerations or notes on decommissioning or destroying sensitive information
    - The last date the asset was reviewed.
- We update our inventory each time a device is added or removed from business-use or periodically throughout the year.

3.2 Information Classification

- When an asset contains confidential or sensitive information, we add the information-classification label 'CONFIDENTIAL' to assets including emails, documents, and systems.

- Whenever an Information Classification label needs to be added, we use the format "**[` INFORMATION CLASSIFICATION `]**" *e.g. Email subject, "[CONFIDENTIAL] Email with employee data".*

3.3 Third-Party Risk Management

- For third-party vendors, such as cloud services providers, we identify who and where to escalate security issues in a security event.
- We escalate security issues to the corresponding third parties within 24 hours.
- Wherever a third-party needs to make security communications or escalations to us, we ensure a dedicated contact is provided.
- We evaluate third-party vendors for their security practices before engagement, such as with cloud service providers like iCloud or Google, requiring contracts that enforce data protection standards. We keep our record of the evaluated data protection standards in the contracts and/or privacy policies supplied by the vendor.
- We assess the security posture of third-party vendors before adoption, including reviewing their certifications (e.g ISO/IEC 27001 or SOC 2) and public vulnerability disclosures.
- We provide our Information Security Policy to subcontractors, and subcontractors must comply with our policy, as per 8. Compliance and Enforcement below. We keep a record of all subcontractors who have received and acknowledged our Information Security Policy in a secure email inbox.
- When needed, subcontractors are required to sign confidentiality agreements, as per 8. Compliance and Enforcement below. We keep a record of all subcontractor-signed agreements in a secure email inbox.
- When we notice a vendor make a security announcement or public security disclosure, we escalate any critical vulnerabilities affecting our systems to our IT Contact within 24 hours.

3.4 Vulnerability Scanning

- We conduct checks for vulnerabilities on our devices, networks, and any devices on those networks. We escalate any detected issues to our IT Contact within 24 hours.
- We don't perform penetration testing against our office networks.
- When we are responsible for the security of a proprietary system, we perform penetration testing after the release of any major changes to that system.

3.5 Security Event Management

- Where available, we enable basic logging of systems such as login attempts, file access history, and other security information, and use the system's default logging retention period. We use this logged security information when any suspicious activity is detected or when assessing a security incident.
- When we identify a security issue or experience a disruption to confidentiality, integrity, or availability of our goods and services, we escalate the security event to our IT Contact via email within 24 hours.
- When we escalate a security event, we provide clear details to the best of our ability. We provide as many of the following as we can:
    - Event description: A summary of what happened, including the nature of the security event (e.g., unexpected access changes to a device, unauthorised access, malware alert, data breach).
    - Date and time: When the event occurred or was first detected, including the time zone if relevant.
    - Source of the event: Where the event originated, such as a specific system, IP address, user account, or device.
    - Affected systems/resources: Details about what was impacted, such as devices, applications, networks, or data assets.
    - Evidence or indicators: Any logs, screenshots, error messages, or other artifacts that support the detection of the event.
    - Actions taken: Initial steps already performed to mitigate or investigate the issue (e.g., turning off a device, resetting credentials).
    - Impacted parties: Any known or possible third-parties or client information that may have been impacted or breached.
    - Any additional context: Relevant background info, like recent changes to the system, known vulnerabilities, or prior similar incidents.

3.6 Incident Response Plan

- We respond to security incidents by following these steps:
    1. Contain: Isolate affected systems (e.g. disconnect them from the network).
    2. Assess: Determine the scope and impact with our IT Contact.
    3. Notify: Inform affected clients or authorities if required (e.g. privacy breaches under Australia's Notifiable Data Breaches scheme or New Zealand's Privacy Act).

4. Recover: Restore systems securely, ensuring the state of all assets is trusted.
5. Review: Discuss lessons learned and update the policy if needed.

- Our leaders are responsible for client notifications and any legal reporting obligations during a security incident.

4. Access Control

4.1 Access Rights and Reviews

- We grant access to systems and data based on the principle of least privilege, ensuring each of us only has what we need for our roles. We review access rights for all users whenever access is added, removed, or updated.
- When anyone with access leaves, we review and offboard their access within 36 hours.

4.2 Authentication

- We never use shared user credentials, unless it is otherwise unavoidable.
- In the event of shared user credentials being created, we notify our IT Contact of the system/service by email.
- We never share our personal credentials.
- We never share a copy of passwords in plain text.
- We use strong passwords that score highly on industry-standard password checkers such as Kaspersky Password Checker (https://password.kaspersky.com/) or similar. A strong password:
    - Contains digits
    - Contains special symbols
    - Contains capital letters
    - Avoids text patterns (such as familiar or commonly used names).
- We never use passwords that are detected in leaked databases.
- We use multi-factor authentication (MFA) across all business systems and authentication methods when available.
- We use Single Sign-On (SSO) when available, allowing employees and subcontractors to access systems with a single set of credentials. Our SSO is configured through a trusted identity provider.

- We enable security alerts in all systems that provide security alerting for authentication, such as suspicious activity.
- We ensure passwords or recovery keys that require storage are stored securely in a password manager and are accessible to leadership if needed for business continuity during a security event.

4.3 Access removal

- When anyone from our team or subcontractors departs, we revoke all their access as quickly as possible and no later than within 36 hours.
- Departing team members or subcontractors are responsible for ensuring that any business data is securely removed from their devices to prevent unauthorised retention.

5. Data Protection

5.1 Data Encryption

- We rely on the native data encryption tools available on device operating systems, such as FileVault on macOS, full-disk encryption (FDE) on Android, or the end-to-end encryption of cloud storage services; and we store confidential data on encrypted volumes wherever possible.
- We use encrypted Wi-Fi networks with a minimum standard of WPA2 (AES encryption) and never use open networks in our offices.
- We foster awareness that un-encrypted confidential information should never be transferred on an open network.

5.2 Data Segregation

- As a business operating in a small-scale digital environment, with no other special operational environments where data is stored, we don't segregate data by environments.
- Wherever possible, we keep client information separate within our assets and systems, to avoid unintentional data exfiltration when sharing adjacent client information, and to avoid unintentional data loss when removing adjacent client information.

5.3 Data Leakage Protection

- We restrict sharing of confidential information to our trusted and reviewed email, chat, and file storage systems, and avoid sharing confidential information on unknown or untrusted channels.

5.4 Backups

- We prefer to use secure cloud services where data is automatically backed up by the cloud.
- We rely on the native backup solutions available on device operating systems, such as Backup and Restore on Windows.
- Where used, we backup data stored on devices to backup solutions, such as Time Machine for Apple devices, and run backups within a 7-day schedule.
- We retain backups indefinitely, unless required by contract or client request.

5.5 Data Disposal and Destruction

- We securely dispose of data no longer needed using deletion and overwrite tools that meet industry standards.
- We review whether data exists that is no longer needed when we are removing access, offboarding a client, decommissioning a device, or when we receive a request to remove information.
- Physical media, such as hard drives, are physically destroyed prior to disposal. This means that we damage physical media and all its physical storage beyond repair, reconstruction, or restoration before disposal.

---

6. Operational Security

6.1 Acceptable Use of Technology

- We install only trusted software.
- When unsure, we request our IT Contact to assess any software for security risks (e.g. malware potential, and vendor trustworthiness).
- The acknowledgement or agreement to our Acceptable Use of Technology is covered by the written acknowledgement of this Information Security Policy, as per 8. Compliance and Enforcement below.

6.2 Patch Management

- We keep our systems and software updated with the latest security patches.
- We prioritise applying security patches to operating systems, applications, and firmware within 21 days of release (or sooner for critical vulnerabilities) to protect against malware and viruses that exploit known weaknesses.
- Our personal devices, known as Bring Your Own Device (BYOD), are updated with the latest security patches, and are the responsibility of the owner to make sure the device is updated.

- End-of-life (EOL) assets are decommissioned securely and replaced as needed.

6.3 Malware Protection

- We install and maintain up-to-date antivirus and anti-malware software on all business-owned devices to detect and remove viruses, malware, and other malicious threats. We report any detected threats to our IT Contact within 24 hours.

6.4 Remote Working

- We perform all remote work on trusted networks, where any Wi-Fi has a minimum of AES encryption such as WPA2.
- We lock all devices and store them securely when not in use.
- We avoid leaving unlocked devices unattended to prevent unauthorised access.
- We avoid leaving devices easily exposed to theft, especially in public locations.
- We avoid printing sensitive data unless a secure shredding method is available.
- We report when a device is lost or stolen to our IT Contact within 12 hours.

---

7. People and Training

7.1 Security Awareness Training

- Our team and subcontractors are responsible for their own Security Awareness Training. We can provide links to free cybersecurity training resources such as:
    - KnowB4's free kits (https://www.knowbe4.com/free-cybersecurity-resource-kits)
    - Cybrary's free courses and hacking training (https://www.cybrary.it/free-content)
    - Phishing.org's guides, quizzes and tests (https://www.phishing.org/what-is-phishing).
- We encourage reporting of suspicious emails to the IT Contact, even if no breach occurs.

---

8. Compliance and Enforcement

- Due to the limited scale of our operations and the low security risk position of the goods and services that we provide, we don't maintain independent information

security related certifications and/or conduct security control audits. We align this policy with the guidelines from the Australian ASD Essential Eight and the New Zealand MBIE Protecting Business Data Guide.

- Our team and subcontractors are required to provide a written acknowledgement of their receipt and understanding of this policy by email. We keep a record of acknowledgements in a secure email inbox.
- When our team or subcontractors require access to information of a client that requires a confidentiality agreement, they sign a confidentiality agreement as a condition of engagement. This agreement outlines their responsibility to protect our business and client data in accordance with this policy. We keep a record of signed agreements in a secure email inbox.
- We issue the latest copy of this policy during onboarding into our business, onboarding into client projects, or when the policy is updated.
- Non-compliance may lead to disciplinary measures, up to termination, particularly if intentional actions harm our business or clients.

---

9. Policy Maintenance

- We review this policy following significant security events, to ensure it remains effective and responsive to emerging risks and requirements.

Suggested additional policies:

If your goods and services include software development, insert these into your policy:

---

*Under **3. Risk Management Controls:***

3.8 Secure Software Development

- We follow secure coding practices that align with OWASP guidelines.
- We perform code reviews (including static analysis) before major releases of our code, to identify security weaknesses.
- We follow a Secure Development Lifecycle (SDLC) to:
    - Plan: We define the scope, objectives, and security requirements of the project and its deliverables
    - Assess: We assess the security risks under the project and determine requirements to mitigate those risks
    - Design: We design the specification of system architecture, incorporating any requirements to comply with our Information Security Policy and the Information Security requirements of the project as provided by the client or identified in our security assessment
    - Implement: We ensure to follow our Secure Software Development policy as we build systems
    - Verify: We test a system or code's security through assurance tests
    - Maintain: We monitor and update systems we have built, following our Patch Management policies.

*Under **4. Access Control**:*

4.4 Secrets Management

9. We use a secrets management tool to securely store, manage, and access sensitive information used by business systems and services (also known as "machine secrets"), including when we use them for managing and deployment infrastructure
10. We never store secrets in plain text
11. We check for any sensitive information in code or other plain text during our verification checks for secure development.

*Replace **5.2 Data Segregation** with:*

5.2 Environment Lifecycle and Data Segregation

- We separate our development and operations to their own environments (e.g Development, Testing, Staging, and Production). We use these separated environments for business systems or proprietary systems through their lifecycle to prevent unauthorised access, data exposure, or accidental manipulation of data integrity.
- Wherever possible, we segregate environments logically and physically, such as segregate them on separate accounts or virtual networks, to prevent unintended data crossover.
- We ensure each of our environments meets our Information Security policies, especially in the areas of Access Rights, Authentication, Patch Management, and Data Disposal.
- We make sure environments are turned off when not in use.
- Wherever possible, we keep client information separate within our assets and systems, to avoid unintentional data exfiltration when sharing adjacent client information, and to avoid unintentional data loss when removing adjacent client information.

If your business has the capacity to resource a more active management of your security risks, insert these into your policy:

---

*Under **3. Risk Management Controls:***

3.9 Business Continuity Planning and Disaster Recovery (BCP/DR)

- We maintain a basic business continuity plan to ensure critical operations persist during disruptions, which details
    - Key contacts to use during a business disruption
    - A set of disruption scenarios and their escalation pathways
    - Key third parties and when they should be notified
    - Standard messaging to communicate to enquiries during a business disruption
    - Key systems and data for business continuity and their recovery priorities

- A clear stance on ransomware events and how to respond to a ransom
- How we test our backup restoration and recoverability and report the results to Our leadership.

*Under **6. Operational Security:***

6.5 Phishing and Social Engineering Protection

- We use email filtering tools to detect and quarantine phishing attempts where available.

6.6 Mobile Device Management

- We ensure mobile devices are configured to protect data, whether business-owned or BYOD, by:
  - Enabling device encryption
  - Enabling lock screens and ensuring lock screens when the screen is turned off
  - Setting PINs with at least 6 digits and using PINs instead of patterns
  - Enabling biometric authentication, such as touch biometrics and face biometrics
  - Installing a trusted anti-virus software
  - Registering the device in our asset inventory
  - Ensure business data can be wiped remotely if the device is lost or stolen.

6.7 Physical Security

- We secure physical assets and workspaces by storing sensitive documents and devices in locked cabinets or rooms when not in use, whether in offices, home offices, or client sites.
- We report lost or stolen physical assets to our IT Contact within 12 hours.
- We make sure that visitors to our offices are escorted and do not access sensitive areas without approval.

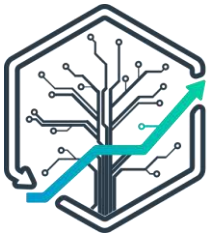
*Under **4.3 Access Removal:***

- When our team members and subcontractors depart, we have them confirm in writing that all business data has been return or securely removed from all devices. We keep a record of all written confirmations in a secure email inbox.

*Under **8. Compliance and Enforcement:***

- We conduct a lightweight security posture review every 12 months, reviewing that all registered and recorded information is up-to-date and compliant with our policy. We add all findings into a report and remediate any outstanding issues within 30 days.

This template was created by DAOS Consulting.



DAOS
Business transformation &
Fractional CxO services

To contact us, go to www.daosconsulting.com
