Information Security Policy

Sensei Policy Document

June 2025

Table of contents

1. Introduction

The Board of Sensei are committed to making Sensei an awesome place to work, whilst also being a high-performing business where all members are able to work with energy and passion. Sensei requires all its members to be courteous, diligent, honest and conscientious. This is because Sensei's performance and sustainability as a business depends on the professional conduct and reputation it has in the marketplace.

Sensei's policy framework is intended to offer guidance to ensure there is clarity, consistency and fairness, so that all members of Sensei can work together to make Sensei an awesome place to work. All members of Sensei have a responsibility to ensure that they have an awareness of Sensei's policies, and to uphold and follow them.

This policy defines the governance and rules around information within Sensei.

All references in this policy to team members, teams, employees, staff, managers, relevant business operations, and to 'Sensei' itself apply to all organisational entities within the Sensei Group, which – at this time of writing – includes Sensei Productivity Pty Ltd (ABN 34 610 828 656) and Altus Pty Ltd (ABN 48 664 209 787) and their related entities.

2. Purpose

The aim of this policy is to establish and maintain the security and confidentiality of information, systems and applications owned and managed by Sensei Project Solutions. The procedures outlined will provide a framework for the detection and prevention of a compromise to information security and protect both our customers and their data but also our reputation.

Sensei is committed to the highest standards of integrity, fairness and ethical conduct, including full compliance with all relevant legal requirements, and in turn requires that all its Board members, officers (including its Chief Executive Officer), managers, employees, volunteers and contractors acting on its behalf meet those same standards of integrity, fairness and ethical behaviour, including compliance with all legal requirements.

There is no circumstance under which it is acceptable for Sensei or any of its employees or contractors to knowingly and deliberately not comply with the law or to act unethically in the course of performing or advancing Sensei's business.

All members of Sensei shall conduct themselves in accordance with their contract of employment and Sensei's Code of Conduct. Any action which is unlawful, dishonest, harmful to others or otherwise against Sensei's principles of responsible business conduct is unacceptable.

3. Scope

The policy applies to all information, systems, applications, locations and employees of Sensei Productivity Pty Ltd and Altus Pty Ltd. For the purposes of this policy, all team members who are currently, or have been historically, employed under the Sensei Productivity Pty Ltd legal entity must adhere to the specifics of this policy.

4. Data and Asset Classification

This section applies to all Sensei information assets, including those involved in outbound and/or inbound information transfers.

It focuses specifically on the classification and control of non-national security information assets, and is primarily intended for the recognised officers responsible for:

➔ implementing and maintaining information assets
➔ incorporating security, integrity, privacy, confidentiality, accessibility, quality and consistency, and
➔ the specific classifications or categorisations of information assets.

For the purposes of classification, an information asset may consist of related information items, grouped together so that broadly similar controls may be applied to the group. Each significant information asset must be classified by the information asset owner based on the confidentiality, integrity and availability requirements of the most sensitive part and business valuable parts of the collection.

4.1. Confidentiality Classification Levels

Classification	Information	Controls
Top Secret	Information assets that require a substantial degree of protection as their compromise could cause serious damage to Sensei, its employees, its customers or other individuals. When compromised these could open ours and other systems up for attack exposing all data. Examples include: ➔ Passwords ➔ Encryption Keys ➔ Application Secrets	Strict access controls e.g. strong encryption routines with long keys; multifactor authentication; safes; access by relevant team members with the highest security clearance (police checks). Electronic media must be destroyed or sanitized.
Strictly Confidential	Information assets whose compromise could cause damage to	Strict access controls e.g. strong encryption routines with long keys; multifactor authentication; safes; access by relevant team members with the

Sensei

ALTUS

	Sensei, its employees, its customers or other individuals. Examples include: ➔ Customer Data (see below) ➔ The names, details and information relating to clients or employees of Sensei;	highest security clearance (police checks) or where authorised by the owner of the data. Electronic media must be destroyed or sanitized.
Confidential	Information assets whose compromise could cause limited damage to Sensei, its employees, its customers or other individuals. Examples include: ➔ Matters of a technical nature, trade secrets, technical data, marketing procedures and information, accounting programs and procedures, financial information, strategic and business plans and like information relating to the business of Sensei or its clients; ➔ Other information which Sensei informs the employee is confidential or which, if disclosed, the employee knows or ought reasonably to know, would be detrimental to Sensei or its clients; ➔ All other information which is imparted to the employee in circumstances which the employee knows or ought reasonably to know that the information is confidential to Sensei or any persons with whom Sensei is concerned.	Strong access controls e.g. standard encryption routines and keys; multifactor authentication; locked filing cabinets

Sensei

ALTUS

Unclassified	Information assets that do not need special security controls or require a classification level. These are not in the public domain, but do not otherwise need to be classified. These information assets require approval from the information owner to be released to the public.	Routine access controls such as needed to authenticated current personnel only.
Public	Information assets which have been authorised by the owner for public access and circulation, such as publications or on web sites.	No requirement.

4.2. Responsibilities

Role	Description	Responsibilities
Asset\Data\Information Owner	Information processed by an information system will have an identified owner. This responsibility will be formally assigned and documented. The Information Owner may delegate some operational responsibilities but will retain accountability.	➜ determine the value of the information within the information system; ➜ determine the statutory requirements regarding privacy and retention; ➜ assign an appropriate security classification label ➜ assign custody of the information; ➜ authorise access to the Information; ➜ specify controls to ensure confidentiality, integrity and availability; ➜ communicate the control requirements to the custodian and users of the information; ➜ develop a disaster recovery or business continuity plan for the information which identifies (i) any potential risks and (ii) vital

		information and communicate this to the Information Custodian.
Information Custodian	Information Custodians are those individuals who control information systems regardless of physical or logical location, storage medium, technology used, or the purpose(s) they serve.	➔ the administration of controls as specified by the owner ➔ evaluating the cost-effectiveness of controls based on the classification attributed by the owner; ➔ implementing physical and/or technical controls; ➔ administering access to information; ➔ ensuring the availability of information by implementing appropriate recovery options based on the business criticality of the information in their possession, as per the disaster recovery or business continuity plan produced by the Information Owner
Information User	Information Users are individuals who have been granted explicit authorisation by the relevant Information Owner to access, alter, destroy, or use information within an information system.	➔ using the information only for the purpose intended by the owner; ➔ complying with all controls established by the owner and custodian; ➔ ensuring that classified or sensitive information is not disclosed to anyone without permission of the owner; ➔ only destroying information accordance with the requirements of the Records Management Policy.

4.3. Classification Process

The recording of the asset, the owner, the classification and the status of controls is to be stored in the Sensei Asset Register.

Step	Name	Description
1	Identify Information System Owners	Responsibility for ensuring that Information Assets have a security classification is authorised by the Information System Owner. Information Assets should be classified by the Information System Owner at the earliest possible opportunity according to the sensitivity of the Information Asset.
2	Identify Information Assets	Identify the Information Asset in accordance with the Security Classification.
3	Assess data vulnerabilities/risks	Perform a risk assessment and consider the vulnerabilities that are attributed to each Information Asset and record risks against the asset in the asset risk register. Relevant data security issues for the Information System Owner to consider might include: ➔ data control ➔ data encryption ➔ blending of data with other customer data ➔ business process if a security breach does occur or if data is damaged or destroyed ➔ data backup frequency/conventions/standards/accessibility ➔ availability of a reliable audit trail.
4	Apply data classification to Information Asset	The highest security classification level determined by the impact assessment must be applied to that Information Asset. Unlike a risk assessment, data security classification is determined by the perceived level of impact to the organisation or individual.
5	Apply controls	Controls are applied as per the classification. Work items are created and assigned as needed to ensure the work gets done to apply the controls according to the classification and risk.
6	Audit logs	To maintain confidentiality and integrity of classified Information Assets a strict audit logging process is desired

		to provide an evidence trail which can be used to investigate inappropriate or illegal access. The auditing mechanisms must be tracked
7	Disposal of Information Assets	To ensure security and confidentiality, the disposal of Information Assets in any form must follow the required controls for the classification.

4.4. Information Handling

1. Sensei employees may only use official information for the work-related purpose it was intended.
2. Unless authorised to do so by legislation, any confidential information must not be disclosed without appropriate approval.
3. Confidential information, in any form, cannot be allowed to be accessed by unauthorised people.
4. Sensitive information should only be provided to people, either within or outside Sensei, who are authorised to have access to it.
5. **Sensei employees have access to information which is not explicitly or reasonably required for day-to-day duties (such as source code to products, information relating to clients that you are not involved with, sales and marketing information, etc.). All Sensei employees are required to make best efforts not to access any information that is irrelevant to day-to-day activities or any information that would be seen as unreasonable in gaining access to.**
6. Caution should be exercised in discussion of personal information between Sensei employees. Normally information should be limited to those who need to know in order to conduct their duties, or to those who can assist us in carrying out our work because of their expertise.
7. Former Sensei employees must not be given access to confidential information
8. Confidential information in Sensei's control:
    a. Shall be collected and used lawfully for specified and legitimate purposes;
    b. Shall be subject to appropriate and adequate organisational, physical and technical security arrangements;
    c. Shall not be retained longer than required for business or legal reasons;
    d. Shall not be stored on any personal or BYO devices

4.5. Customer Data

For this policy, "customer data" is defined as:

- Sensei Solution Component: The Software as a Service (SaaS) or licenced, instantiated copy of a Sensei Solution component.
- Customer: The company or organisation that represents the end-users of a Sensei Solution.
- Partner: The reseller or authorised agent to sell, deploy and support the Sensei Solution Component on Sensei's behalf.
- Client Care Admin: The Client Care Delivery Director, Client Care Team Leader(s) or Client Care team member(s) who have been authorised by the Client Care Delivery Director.
- Solutions Administrators: A small group of dedicated administrators responsible for Security Incident Response and BCP execution.
- Customer Data: Any data or artefacts supplied by the customer that are stored within Sensei Solutions Components.
- Shared Account. An account where the human responsible for the actions of the account are ambiguous.

5. Physical Asset Management

Asset management is basically the IT part of the asset. It will cover the lifecycle of how the asset will be taken onboard, installed, maintained, managed and retired. The lifecycle can have major parts defined:

5.1. Asset onboarding

Sensei provides the option to all employees to be provided with a company laptop or to BYOD and be reimbursed.

All company owned devices need to be approved by the state manager. Physical infrastructure is not to be procured or operated by Sensei except under special circumstances; Sensei operates under an Azure cloud-first strategy and currently maintains no physical servers.

Sensei resources are accessed via public network infrastructure with no physical local networks or domains maintained. Operational security is provided by ensuring that cybersecurity best practices are implemented and adhered to end-to-end by all Sensei employees.

All Sensei employees have 'local administrator' rights on personal computers, however are encouraged not to use this as the primary account for additional security.

Sensei employees must associate their work device with Sensei via Azure Active Directory and Mobile Device Management, which enforces security features such as Antivirus and Antispyware software and automatic workstation locking.

Cloud infrastructure is provisioned under the authority of the individual departments within Sensei's Azure subscription and are listed therein. The owner of the device is hence responsible for the installation and configuration of the device.

5.2. Asset Inventory

Sensei maintains an asset inventory of all physical assets that store or interact with information assets, such as laptops and servers. As part of the inventory we allocate an owner, outline what data is stored or processed and how it is secured inline.

Sensei has real-time access to a list of devices in Azure Active Directory which have been connected to Sensei resources via Mobile Device Management. Each device is listed along with the user who is using it. This includes not just windows devices such as laptops, but also mobile devices such as iPhones and iPads.

Cloud infrastructure such as virtual servers and virtual networking services are catalogued automatically in Azure.

5.3. Asset Deallocation/Retirement

Asset deallocation and retirement occurs when an employee ceases employment, an employee receives a new laptop (every 3 years), or a server is deemed obsolete and no longer required.

All end-of-life or retired devices must be securely wiped to remove all data before disposal. Physical destruction is required if secure wiping is not feasible. Follow environmentally responsible recycling practices for all discarded devices. For BYOD situations the company and the user will remove their laptop from Mobile Device Management which will prevent the device from accessing company resources. As part of the offboarding process all company data needs to be deleted from the device.

5.4. Annual maintenance/warranty

For company owned devices, level 1 support is provided by the Client Care team, while the warranty will be provided by the manufacturer.

General maintenance and patch management is the responsibility of the device owner.

Windows Updates are enforced as automatic by device policy.

For cloud infrastructure such as virtual servers, the maintenance and patch management is the responsibility of the user or team that owns it.

6. Access Control Principles

This section applies to Customer Data regardless of the physical or administrative ownership of the data. This includes both uniquely created data and data extracted or aggregated from other Customer owned systems.

It specifically excludes data managed by the Customer in non-Sensei systems or components.

It applies to the handling of Customer Data by direct Sensei employees, specifically excluding all Customers, Partners and Microsoft Employees.

6.1. Guiding Principles

➔ **Need to know**. Users will be granted access to systems that are necessary to fulfil their roles and responsibilities.
➔ **Least privilege**. Users will be provided with the minimum privileges necessary to fulfil their roles and responsibilities.

6.2. Access Procedures

➔ Access to information shall be restricted to authorised users who have an actual business need to access and process the information. This needs to a justified need as per their role and authorised by the customer if customer related.
➔ Requests for additional access privileges to Customer Data originating from within the Customer organisation that can be enacted through the relevant self-service UI are excluded from this policy and are subject to the Customer's own IT Policies and procedures for authorised access.
➔ Requests for additional access privileges to Customer Data originating from within Sensei must be formally documented via a Client Care ticket and appropriately approved by Client Care Admin before granting access.
➔ Requests for special accounts and additional privilege to access Customer Data (such as Partner accounts, Test accounts) must have a documented originating Customer email/Client Care ticket.
➔ Where possible, technical mechanisms will be put in place to enable the automatic expiry of Customer Data access at a pre-set date. More specifically.
  o When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
  o Sensei user accounts participating in a Customer project will have access removed at the completion of the Project.
➔ Access rights will be immediately disabled or removed:
  o When the employee is terminated or ceases to have a legitimate reason to access Customer Data. See Sensei Offboarding policy.

- o If the business has reasonable grounds to suspect a breach of this Information Security Policy.
- o If the business has reasonable grounds to suspect the relevant employee's account has been compromised or is otherwise being utilised to facilitate a security breach or cyber event.

➔ A verification of the user's identity and the legitimate need for Customer Data access will be performed by Client Care Admin prior to granting access.

➔ Existing user accounts and access rights will be reviewed at least annually by Client Care Admin to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:
- o An active account assigned an employee that no longer work for Sensei. This is a safety check for the proper functioning of the Offboarding policy.
- o An active account with access rights for which the user's role and responsibilities have changed over time that no longer have authority/responsibility/need to access Customer Data.
- o System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) are granted to a user who is a not a member of Solutions Administrators or Client Care Admin.

➔ All access requests for elevated access to Customer Data are documented via Client Care ticket.

➔ While not having direct permission to Customer Data, it is acknowledged that the Solutions Admin team members must maintain administrative control of all systems in order to facilitate the adequate execution of the Security Incident Response Plan and regional BCPs.

➔ When dealing with Customer Data all employees will do so from locations within Australia unless special consent is sought and approved by the relevant customer.

6.3. Administrative accounts

➔ All Administrative accounts within Client Care Admin and Solutions Admin that can change the security settings or performance settings of a system must have Multi-Factor authentication enabled.

➔ To have Administrative access to our systems, users must pass a Policy background and security check.

6.4. Non-Administrative accounts

➔ All accounts within Sensei must have Multi-Factor authentication enabled.

6.5. Shared Accounts

➔ Access to Customer Data shall not be granted to any Shared Accounts, where the human responsible for the actions of an account are ambiguous.

➔ No Shared Accounts will be created, or existing account repurposed as Shared for the purposes of multiplexing access to Customer Data.

➔ If Client Care or Solutions Admin becomes aware of a Shared Account, access to Customer Data will be revoked immediately.

6.6. Shared Service Account Usage and Delegated Responsibilities

The purpose of this policy is to ensure that shared service accounts are not used within our organisation and that a delegated person is accountable and responsible for the ownership and management of the mentioned services within this policy. This policy aims to enhance security, accountability, and proper management of the Power Platform and Microsoft Fabric services.

This policy applies to all employees, contractors, and third-party users who manage or interact with the following services:

➔ Power Platform (including flows, power apps, and power platform connections)
➔ Data flows
➔ Power Automate
➔ Power BI
➔ Power BI Reports
➔ Microsoft Fabric

Policy Statement

Prohibition of Shared Service Accounts

➔ Shared Service accounts shall not be used for managing or owning any service in the Sensei tenancy including the above-mentioned services.
➔ All connections, configurations, and administrative tasks must be performed by individual user accounts with appropriate permissions.

Delegation of Responsibilities

➔ Each service within the Power Platform family and Microsoft Fabric must have a designated owner who is accountable and responsible for its management.
➔ The designated owner must be an individual employee who is adequately trained and authorised to handle the responsibilities of the service.
➔ Ownership includes, but is not limited to, the following:

➔ Connection ownership and management
➔ Monitoring and maintaining data flows
➔ Managing Power Apps and Power Automate flows
➔ Overseeing Power BI reports and connections

Accountability and Responsibility

➔ The designated owner of each service is responsible for ensuring the security, compliance, and optimal performance of the service.
➔ The designated owner must regularly review and update the connections and configurations to ensure they meet organisational standards and security policies.
➔ The designated owner must promptly address any issues or incidents related to the service and report them to the appropriate stakeholders.

Roles and Responsibilities

IT Security Team

➔ Ensure that no shared service accounts are used for the designated services.
➔ Conduct regular audits to verify compliance with this policy.

Service Owners

➔ Accept accountability and responsibility for their designated services.
➔ Maintain and manage connections, configurations, and data flows.
➔ Ensure compliance with organisational security policies and standards.

Employees and Users

➔ Adhere to this policy and avoid using shared service accounts for the specified services.
➔ Report any violations or issues related to this policy to the IT Security Team.

Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Violations of this policy will be investigated, and appropriate corrective actions will be taken.

Review and Revision

This policy will be reviewed annually and revised as necessary to ensure it remains relevant and effective in addressing the organisation's needs and security requirements.

6.7. Partner Accounts

➔ The use of security features in Sensei Solution Components by Partners and their subsequent Customers are the responsibility of Partners and Customers respectively, pursuant to their own IT policies for authorised access.

6.8. Exceptions

Exceptions to the principles in this policy must be documented and formally approved by the Engineering Director. Policy exceptions must detail:

➔ The relevant Sensei Solutions Component and Customer Data exposed.
➔ A reasonable explanation for why the policy exception is required.
➔ Any risks created by the policy exception.
➔ Evidence of approval by the Engineering Director.

7. Password Management

To prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the company network. The company's strong password policy is:

- ➔ The utilisation of Dashlane for all Sensei-related password management (please see our I.T. Support and Security Officer for relevant access).
- ➔ Passwords should be changed on first login
- ➔ Passwords must be at least eight (8) characters and a combination of upper and lower-case letters, numbers and symbols
- ➔ New passwords can't be one of 15 previous passwords
- ➔ Non expiring passwords with high complexity.
- ➔ All user accounts provided by Sensei will use multi-factor authentication via a validated personal device.
- ➔ Number of failed logon attempts allowed: 5 within 2 minutes
- ➔ Account lockout duration: 30 minutes
- ➔ Reset failed logon attempts count after 30 minutes
- ➔ Sensei team members are encouraged to generate strong passwords using Dashlane.
- ➔ Sensei team members are encouraged to use a pass-phrase rather than a single password.
- ➔ Password managers remain a best practice for individuals as much as organisations, and Sensei team members must utilise the password managerDashlane for all Sensei-related password management.

> ℹ It is now accepted industry best practice not to force users to change their passwords. See Microsoft Research Whitepaper for details.

7.1. Storage

Sensei and Customer credentials should be stored in a secured location, with the backend encrypted appropriately and backed up to the cloud.

Never reveal your password to others. Your login credentials protect information as valuable as the money in your bank account. Nobody needs to know them.

Passwords should not be written down on physical media (e.g. on a post-it note, in the back of a notebook, on a card in your wallet, etc.).

Product secrets and keys are stored and managed for the solution via Key vault and Dashlane where appropriate.

7.2. Exchange

When exchanging passwords with 3rd parties as is occasionally necessary, preferentially utilise secure end-to-end encrypted channels where available. Intra-tenant Exchange Online email falls into this category, however email to external parties does not.

Use Dashlane's 'share' feature to securely share credentials with both Dashlane and non-Dashlane users.

In the case where an end-to-end encrypted channel is not available ensure the username and password are sent to single recipients via separate communications channels, e.g.: Username via email, password via SMS.

8. Change Management

This section defines the governance guidelines around changes to our solutions products and production environments.

Change Management is the process of requesting, analysing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The Change Management Process begins with the creation of a Work Item within Sensei Azure DevOps (VSTS) installation. It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

- ➔ Environmental releases go through our Continuous Integration and Zero Downtime Deployment procedures.
- ➔ Releases to any environment must be approved by an authorised user.
- ➔ All releases are propagated by the Visual Studio release management system.
- ➔ Regular code reviews are conducted by peers on changesets before deployment.

While it is impossible to perform regression testing on all customer scenarios, essential practical testing and monitoring is performed to ensure changes do not produce adverse effects.

The scope of these procedures is restricted to the areas of code/product and the related infrastructure.

8.1. Code/Product Changes

Step	Description
1	Work item created in Work Item Tracking Tool
2	Work Item reviewed and approved by team (including Product Owner)
3	Work done ➔ Database changes should be backward compatible ➔ Unit/Integration tests written where appropriate
4	Code Review (via pull request) on change sets (linked to work items)
5	Tested in Latest by an alternate user
6	Regression/unit tests pass
7	Rollback/Rollforward strategy agreed and documented ➔ Tested if determined necessary by the team
8	Customer Notification need evaluated
9	Deployed by VSTS release management ➔ 1st Release (validation ring) where available ➔ Staging Release

ALTUS

	o Ideally production scenarios are tested ➔ With approval by authorised users onto Production o If deployment fails, then rollback/rollforward strategy enacted ➔ Notification to Teams Prod change log

8.2. Infrastructure Changes

The procedure covers changes to Azure Infrastructure including IaaS and PaaS, as well as any production configuration changes to our systems wherever they are.

Step	Description
1	Work item created in Work Item Tracking Tool
2	Work Item reviewed and approved by team
3	Change performed by authorised users (access is as needed and restricted)
4	Change is tested where possible in Latest environment
5	Change performed in Staging and Production
6	Comment added to Teams Channel shared with Client Care including what and why (who and when is recorded automatically)
7	Azure audit log records all changes additionally

8.3. Monitoring

Post change monitoring is performed by the solutions and Client Care teams via

➔ Application Insights
➔ Azure Dashboards
➔ Azure Alerts

9. Incident Management

The following section outlines the Incident and Breach response and management plan.

9.1. What is a data breach?

A data breach occurs when personal information that Sensei holds is subject to unauthorised access, or disclosure or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. We should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

➔ loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
➔ unauthorised access to personal information by an employee
➔ inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
➔ disclosure of an individual's personal information to a scammer, because of inadequate identity verification procedures

9.2. Consequences of a data breach

Data breaches can cause significant harm in multiple ways.

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of harm include:

➔ financial fraud including unauthorised credit card transactions or credit fraud
➔ identity theft causing financial loss or emotional and psychological harm
➔ family violence
➔ physical harm or intimidation

A data breach can also negatively impact Sensei's reputation for privacy protection, and as a result undercut Sensei's commercial interests.

Sensei can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that Sensei takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in Sensei's personal information handling capability.

9.3. Response Plan

At all stages of the response process decisions and notes need to be documented and stored in the intranet appropriately.

Step	Name	Description
1	Detect	A breach has been internally/externally observed, suspected or detected through monitoring and immediate responsible team notified e.g. Solutions, Client Care.
2	Contain	Contain a suspected or known breach where possible. Take immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.
3	Escalate	The incident should be escalated to department heads and the CEO. If necessary, at this stage in the procedure, we may like to engage a third party for advisory services and / or to assess the severity of what's taken place. At time of writing, our contacts for Cyber CX is as follows: Jordan Jurek | Security Consultant, Security Testing & Assurance (ST&A) | 0433 596 629 | CyberCX Sarah Taylor | Account Manager | SA m: 0407 277 183 | e: sarah.taylor@cybercx.com.au | www.cybercx.com.au Level 2, 136 Greenhill Road, Unley, SA 5061
4	Assess	The response team should be formed and establish if an event is an incident and what the potential impact of the breach is to owners of the information.

		If there is uncertainty as to the impact, then an assessment must be planned and performed: 1. Plan: initiate a plan and assign a team or person to execute it 2. Investigate: gather the relevant information about the incident to determine what has occurred 3. Evaluate: make an evidence-based decision about the risk of harm This must be completed as a matter of priority. At least to the point where the decision on notification can be made within the obligated timeframe. In your assessment of a data breach, consider: ➔ the type or types of personal information involved in the data breach ➔ the circumstances of the data breach, including its cause and extent ➔ the nature of the harm to affected individuals, and if this harm can be removed through remedial action
5	Take Action	Beyond containment, take simultaneous steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is assessed or changing access controls on compromised customer accounts before unauthorised transaction can occur. If remedial action is successful in making serious harm no longer likely, then notification may not be required.
6	Notify	If the breach is likely to result in a risk to the rights and freedoms of individuals or corporations, Sensei is obligated by law to notify the affected parties or appropriate supervisory authority within the appropriate timeframe for their region. Sensei must prepare a statement outlining: ➔ A description of the breach ➔ The kind/s of information concerned ➔ Recommended steps for individuals One of the following options should be performed: 1. Notify all individuals directly 2. Notify only those individuals at risk of serious harm 3. Release the statement on the Sensei web site and publicise it

Sensei

ALTUS

7	Review	The response team will review the incident and take action to prevent future breaches, including:
		
		→ Cause of the breach
		→ If the response plan was executed effectively
		   o What was done well
		   o What was not done well
		→ Prevention plan including changes to systems
		→ Establish pro-active audits to ensure plan is implemented
		→ Revise this policy and other company procedures
		→ Update staff training

9.4. Response Team

When an incident occurs the following team members should be assembled and/or consulted.

→ Team leader/Project Manager
→ Sensei CEO
→ Solutions senior staff member
→ Client Care senior staff member
→ Relevant technical specialist
→ Human resources – to advise if the breach was due to staff actions
→ Marketing – to assist in communicating the breach
→ Legal advisor (external to Sensei)
→ Cyber advisor (external to Sensei)

10. Risk Management

The purpose of this section is to provide guidance regarding the management of risk to support the achievement of Sensei's objectives, protect our staff, customers and business assets and ensure financial sustainability.

This policy has been developed to;

➔ Support effective decision-making;
➔ Ensure a consistent and effective approach to risk management;
➔ Formalise the commitment to the principles of risk management and incorporating these into all areas of Sensei; and
➔ Foster and encourage a risk-aware culture where risk management is seen as a positive attribute of decision-making rather than a corrective measure.

10.1. Governance structure

The risk governance structure of Sensei is as follows

Board	Provides policy, oversight and review of risk management
Chief Executive Officer	Drives culture of risk management and defines and improves risk management policy, strategy and supporting framework
Managers	Ensure staff in their business units comply with the risk management policy and foster a culture where risks can be identified and escalated
Staff and Contractors	Comply with risk management policies and procedures

All staff are responsible for raising and highlighting risks when they become apparent.

10.2. The Sensei framework

The Sensei risk management framework has 5 iterative phases:

Phase	Name	Description
1	Recognition	New risks are raised in the appropriate risk register for the department or company. It is important to track the context of the risk, so it is clear what the scenario is and why it is a risk.

Sensei

ΛLTUS

2	Assessment	The department or management team will assess consequences and likelihood of each risk.
		Here analysis is done that investigates and draws upon:
		→ The information on risks generated during risk identification → The effectiveness and reliability of controls → Additional information from the statement of context → Supporting statistical data, results of predictive modelling or expert judgement → The risk criteria developed during establishing the context.
		The aim of risk analysis is to gain an understanding of the nature of each risk, including the magnitude of its consequences and their likelihoods, and therefore to derive the level of risk.
		Risk analysis enables each risk (or group of risks when considered in the aggregate) to be evaluated to determine whether risk treatment is needed.
3	Evaluation	Risk evaluation uses the information generated by risk recognition and assessment to make decisions about whether each risk falls within an Sensei's risk criteria and whether it requires treatment.
		Sensei specify the actions required by managers for risks at each level of risk and the time allowed for their completion. They also specify which levels of management will be permitted to accept the continued exposure and tolerance of certain levels of risk.

| 4 | **Management** | The risk is assigned and dealt with via one or more of the following steps:

 ➜ Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
 ➜ Accepting or increasing the risk to pursue an opportunity
 ➜ Removing the risk source
 ➜ Changing the likelihood
 ➜ Changing the consequences
 ➜ Sharing the risk with another party or parties (including contracts and risk financing)
 ➜ Retaining the risk by informed decision |
| 5 | **Monitoring** | The risk is monitored for impact and reviewed again in the next cycle |

Once implemented, the risk will be managed by the CEO and reported to the Board in regular (quarterly) updates. High priority or severity risks will be escalated to the next weekly management or department meeting.

10.3.   Vulnerability Disclosure Program

Sensei strongly believes that the security researcher community can help us make our products and customer data more secure. These days security researchers and hackers play an important role in discovering vulnerabilities that slip through the development process.

Security researchers and white hat hackers that have found vulnerabilities in our products and services are encouraged to let us know about the vulnerability by emailing us at helpdesk@sensei.cloud.

We promise to respond to any submitted vulnerability within 72 hours.

At this point we do not have formal bounties available to reward researchers, we will however be keen to work with anyone who discovers a vulnerability and depending on the magnitude of the issue will look to show our gratitude in some form.

Some rules to follow when looking for vulnerabilities:

→ Only test against your own data and with your own accounts.

→ Do your best to avoid research that violates customer privacy or destroys data.

→ If you discover customer data while researching, or are unclear if it is safe to proceed, please stop immediately and contact us.

→ Be reasonable with automated scanning methods so as not to degrade services

→ Reports from automated tools or scans should include additional information demonstrating how the vulnerability can be exploited

→ Refrain from disclosing the vulnerability until we have addressed it

The scope of the tests is somewhat unrestricted and can include any of our publicly accessible websites and services, whether they are authenticated and secured or not.

11. App Permissions Governance

The purpose of this section of the policy is to manage and govern enterprise application permissions in Microsoft Entra ID (formerly Azure AD), ensuring that access to corporate data is secure, justified, and aligned with the principle of least privilege.

This section of the policy applies to all enterprise applications registered in Microsoft Entra ID that request or have been granted delegated or application permissions to access organisational data.

11.1. Inventory Management

➜ All enterprise applications in Microsoft Entra ID must be inventoried and reviewed regularly.
➜ Applications must be tagged with an owner, business function, and intended use.

11.2. Consent and Permissions

➜ Admin consent must only be granted with documented business justification.
➜ Application permissions (daemon/service apps) must undergo a higher level of scrutiny due to their elevated access.
➜ Delegated permissions must be scoped to individual users unless otherwise justified.
➜ All consent grants (user or admin) must be recorded and reviewed.

11.3. Access Review

➜ App permissions must be reviewed at least annually to remove unused or over-permissioned apps.
➜ Owners must validate app necessity, scope of permissions, and usage status.

11.4. Least Privilege Enforcement

➜ Applications must only be granted the minimum required permissions to perform their function.
➜ Avoid granting wide-scope permissions like *.Read.All or *.Write.All unless critically necessary and approved.

11.5. Approval Workflow

➜ All admin consent grants must go through a formal approval workflow.
➜ Approvals must be recorded and retained for audit purposes.
➜ Conditional Access or Just-in-Time (JIT) access should be enforced for sensitive applications.

Sensei

ALTUS

11.6. Third-Party Risk Management

➜ Third-party apps must undergo vendor risk assessments, including checks for data residency, data retention, and support for Microsoft security controls.

11.7. Training & Awareness

➜ Application owners and IT managers must be trained on the risks and governance of app permissions.
➜ New app onboarding must include a permissions review step.

11.8. Audit Readiness

➜ All actions and reviews related to app permissions must be logged and auditable.
➜ A documented remediation and escalation path must exist for over-permissioned or risky applications.

12. Clean Desk Policy

In general, Sensei uses hot desks at all its offices and additionally has shared office spaces in Melbourne with another company. Due to this Sensei has the following strict policy to Desk and public spaces.

The following policy is in place to prevent unauthorised access by Sensei or non-Sensei individuals:

➔ All unattended devices will be locked. If left idle for 5 minutes all devices will auto lock
➔ All confidential data when printed will be stored securely and not left unattended on desks or in the printer at any time
➔ The printer area and meeting spaces need to be kept clean, especially of confidential data
➔ On customer site, or shared office environments, all portable devices will be secured in lockers and not left on desks after hours.

Random checks by management and office staff will be enforced.

13. Data Support & Operations

In this section we cover data protection, storage and movement policies.

13.1. Basic Data Protection Requirement

Systems holding personal information (broadly, data collected from customers) must be protected in alignment with Sensei's corporate standards and industry best practice. Specifically, the systems must operate:

- ➔ Up to date anti-malware protection
- ➔ A firewall
- ➔ Encryption at rest and in transit
- ➔ Be appropriately patched
- ➔ Have bit locker activated
- ➔ Be enabled for remote wipe

13.2. Storage Media and Backup

Backups of data will be encrypted in line with industry best practices and hosted in an area of physical security to protect against unauthorised access. Backup media must always be stored in one of the following areas:

- ➔ A cloud hosted service protected by the user's personal work account
- ➔ A device protected by the user's personal work account
- ➔ A secure approved data centre
- ➔ Inside locked furniture within the company offices

At time of writing, Sensei's sole backup provider is Microsoft (Azure Backup, OneDrive, SharePoint, and Exchange Online backups).

Azure Backup service provides simple, secure, and cost-effective solutions to back up data and recover it from the Microsoft Azure cloud. Given the presence of cloud-based solutions such as OneDrive, SharePoint and Exchange, Sensei team members are required to ensure all business critical files and folders are backed-up to one or more of these solutions.

Sensei will consider alternative backup suppliers or strategies, but only those which do not increase our security vulnerability or our overall data footprint.

More information on Microsoft's Azure back-up strategy can be found here: https://learn.microsoft.com/en-us/azure/backup/backup-overview

13.3.   Data Movement

➔ Data is to be transferred only via business provided trusted transfer mechanisms. As per data classification it must be secured and encrypted where appropriate.

➔ Any information being transferred on a portable device (e.g. mass storage device or a laptop) outside of Sensei or across a public network must be encrypted in line with industry best practices.

➔ Email should be avoided unless initiated or insisted on by the customer. A secure file share is preferred.

13.4.   External Storage Devices

Storing sensitive company or customer data on removable media/storage devices should be generally avoided wherever possible, and only employed temporarily as a last resort.

While external storage devices (such as portable hard drives, USB sticks and memory cards) are permitted for use at Sensei, all staff members should take precautions these devices do not become compromised with any malicious software or viruses which may pose a threat to Sensei. Also, staff should ensure that any USBs, memory cards, or portable hard drives utilised should be under their full control / ownership at all times.

Sensei promotes the following best practices when it comes to external storage devices;

➔ Ensure anti-virus solution(s) are maintained on your device that will actively scan for malware when any type of removable media or storage device is connected.

➔ Ensure that all removable media and storage devices are encrypted. This will protect data from unauthorised users should the device be lost or stolen.

➔ Never connect found media or devices to a PC. Give any unknown storage device to Client Care or Product Development personnel.

➔ Always apply new passwords before and after every business/personal trip where company data is being utilised on removable media or storage device.

➔ Never disclose the passwords used with removable media or storage device to anyone, except where compelled to by the current legal jurisdiction.

➔ Disable the Autorun and Autoplay features for all removable media or devices. These features automatically run when plugged into a USB port or drive.

➔ Keep your personal and business data separate. Do not store company data on your personal external device.

➔ When you have finished transferring sensitive data from removable media or device, be sure to securely delete it from that external storage device.

➔ When the lifespan of a removable media or storage device is over be sure to sanitize the media/storage device destructively (so it cannot be repaired to retrieve the data) or if re-purposing/changing ownership of the removable media/storage device that it is prepared in compliance with NIST 800-88 standards for media sanitisation.

➔ Team members should consider the benefits of encrypting their USB devices; review the Microsoft information located here: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/how-and-why-to-encrypt-usb-flash-drive

14. Acceptable Internet Usage Policy

The company defines acceptable business use as activities that directly or indirectly support the business of Sensei. The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading, social media or game playing. Team members are not to access certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to:

➔ Illegal websites
➔ Websites promoting or engaging in gambling activities
➔ Websites containing pornographic material
➔ Other websites that when reasonably considered, may cause offence, upset or distress to other employees.

Devices may not be used at any time to:

➔ Store or transmit illicit materials
➔ Store or transmit proprietary information belonging to another company
➔ Disclose non-publicly available or sensitive information belonging to Sensei or it its customers
➔ Harass others
➔ Engage in outside business activities

When posting on social media sites in a private capacity, Sensei team members must behave in a way that upholds the values and reputation of the Sensei. Team members must not discuss or disclose Sensei information that is not publicly available, whether confidential or not. If team members comment on Microsoft, Industry or Sensei related matters in a private capacity on social media sites, they must avoid any reference to their employment by Sensei, and also avoid implying that Sensei endorses their personal (private) views.

15. Antivirus and patch management

15.1. Laptops and BYOD

All Windows devices that are connected to corporate data including BYOD are enforced via MDM to have:

→ Windows Defender Antivirus
  o automatically updated daily and scans regularly
  o real time protection
→ Device Encryption via BitLocker

The standard operating system is Windows 10 (or above) which has automatic updates enabled to make sure they are patched and up to date. This can't be disabled.

All Apple Macintosh machines must have an additional anti-virus product installed and maintained up to date by the operating user.

15.2. SaaS and PaaS

Where possible Sensei has a policy to use SaaS (Software as a Service) applications and Azure PaaS (Platform as a Service) to host the services we provide. This means that antivirus and patch management is handled for us by the service provider.

15.3. Servers and VMs/IaaS

For the limited servers we host and the VMs we run in Azure IaaS (Infrastructure as a Service), in order to maintain availability of the servers during business hours, we have manual schedule to remind us to install the updates and restart the machines.

The reminder creates work items in our work management system and the team completes the task as part of the flow of work.

15.4. Software Dependencies and 3rd Party Components

For all the software components we develop in house we have the following guidelines in place for the product team.

→ Important/critical vulnerability bulletins will be monitored and patched urgently as a matter of priority above existing work

➔ High impact vulnerabilities are queued as part of our current workload and addressed by the next available team member

➔ Medium/low impact updates are to be reviewed:
  o nonbreaking changes may be merged with other updates as part of the general release cycle
  o breaking changes will be added to the backlog and queued/prioritised as part of the regular process.

16. Physical Security

This section covers the physical security controls and operational procedures at Sensei.

General controls across all the Sensei offices include.

- → The front door is monitored by office staff to greet visitors
- → Visitors cannot be in the office unaccompanied
- → Fire alarms and fire wardens
- → Lockers available to secure personal items

Physical security varies in the different offices. In general, the front door is monitored by office staff to greet non staff members.

- → **Melbourne**: Sensei's Melbourne office is located on the 15th floor of an 18 storey building. The lifts to the 15th floor are locked down between the hours of 5.00pm and 7.30am each evening/morning, 24 hours on weekends, and 24 hours on public holidays. Access to the building itself is locked down from 5.30pm until 7.30am each evening/morning, 24 hours on weekends and 24 hours on public holidays. Access to both the building itself and the floor during these hours requires a swipe card, a register for which is managed (each fob has a unique identifier, which is tied to an employee as they come on board. Lost fobs are immediately deactivated by the Property Manager). Access to the floor via the fire escape also requires a security fob. Physical files are kept under lock and key.

- → **Brisbane**: Sensei's Brisbane office is located on the 9th floor of a 13 storey building. The lifts to the 9th floor are locked down between the hours of 6pm and 6.30am each evening/morning, 24 hours on weekends and 24 hours on public holidays. Access to the Sensei office space is via a physical key, which are issued to new Sensei staff members upon their commencement. No physical files are located in this premises.

- → **Sydney**: As of February 2025, Sensei has decommissioned its Sydney office in favour of a collaboration space called 'Hub' (located in Sydney's CBD). All of the Hub coworking spaces have 24/7 CCTV footage, secure passes for access to the space, private offices and meeting rooms, and a welcome desk attended by a concierge from 8am – 5pm, Monday – Friday.

- → **Adelaide**: Sensei's Adelaide office is located on the third floor of a city-based, commercial 14-storey location. There is a key card to gain access to the front and rear door of the building on the ground floor. The same keycard is required to access the building after hours. To gain access to level 3, there are lifts which are open between 8am and 6pm. Access outside of these hours requires a key card. The lifts are also closed down to all except those with a key card on weekends and public holidays. Sensei team members' key cards provide access to the Sensei office, but no other tenancies within

the building. The building is monitored after hours by an external security company, who conduct periodic checks during close-down periods. Special access requests are required for access during longer shutdown periods. All physical files are kept under lock and key.

17. Remote Work Procedure

With multiple offices and employees working on projects remotely in other states it is a common practice at Sensei to work remotely from their place of residence.

To access company cloud services such as email, the device in use needs to be associated to the workplace and in turn protected by data encryption and antivirus.

All staff are obliged the follow the clean desk policy as described in this document even when not in the office to protect sensitive data.

All cloud Azure Data services are protected by firewalls, and to access them, Sensei staff are required to maintain their single IP address in the exception lists to avoid the list getting stale. This process will be performed by the employee themselves if they have the clearance, or via an authorised person in the Solutions or Client Care team.

It is the employee's responsibility to ensure their network is secure and protected by necessary encryption and firewalls.

Staff are required to seek written permission from the customer if working outside the agreed border / scope of data sovereignty for the engagement.

18. Security Awareness Training

Information security awareness training is available covering this policy, in particular:

- ➔ the collection and maintenance of data
- ➔ data quality
- ➔ confidentiality
- ➔ privacy
- ➔ acceptable use of systems and social media
- ➔ physical security

All staff need to have completed this training including a small test afterwards. This is auditable and is part of the induction process, to ensure staff are up to speed from the time they start.

Once a year staff should be run through a refresher of the training.

19. Responsibilities, Rights and Duties of Personnel

Ultimate responsibility for information security rests with the CEO of Sensei. This goes in hand with providing the time, means and resources to enforce and follow the policy.

All staff shall comply with the above procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Each member of staff shall be responsible for the operational security of the systems they use.

Each system user shall comply with the security requirements that are currently in force and shall also ensure that the confidentiality of the information they use is maintained to the highest standard.

20. Information Security Review Schedule

All policies are currently checked monthly by the CEO. This policy will be reviewed in detail by the CEO of Sensei at least annually in-line with the policy review policy. As part of the review, a representative of the Altus product team and Client Care will be involved to ensure it is up to date and accurate.

21. Related Legislation

- The Australian Privacy Act 1988 - https://www.legislation.gov.au/Series/C2004A03712
- The Australia Privacy Act Amendments
    - https://www.legislation.gov.au/Details/C2006C00121
    - https://www.legislation.gov.au/Details/C2004A00748
    - https://www.legislation.gov.au/Details/C2017A00012
- General Data Protection Regulation (EU) - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

22. Authorisation

Andy Neumann
20th December 2019
Reviewed July 2021
Reviewed May 2022
Revised February 2023
Revised October 2023
Revised June 2024
Revised September 2024
Revised February 2025
Revised May 2025
Revised June 2025

Annexure 1: Guest Account Multi-Factor Authentication (MFA)

This section of Sensei's Information Security Policy is established to enhance the security of our organisation's systems and data by ensuring that all guest accounts have Multi-Factor Authentication (MFA) enabled. MFA adds an extra layer of security by requiring users to provide multiple forms of verification before accessing our systems and sensitive information. This policy applies to all guest accounts granted access to our organisation's resources and systems.

Policy Guidelines

1. **Scope:** This policy applies to all guest accounts, including but not limited to vendors, contractors, partners, clients, and any other external individuals or entities that require access to our organisation's systems and data.

2. **MFA Implementation:** All guest accounts must have MFA enabled before being granted access to our systems and resources.

3. **MFA Methods:** Guest accounts should use at least two of the following MFA methods:

    a. Something you know (password): A strong, unique password must be set for each guest account.

    b. Something you have (e.g., smartphone, token): MFA can be achieved through authentication such as Microsoft Authenticator.

    c. Something you are (e.g., biometrics): If applicable, biometric authentication methods (e.g., fingerprint, facial recognition) can be used in combination with other MFA methods.

4. **Enrolment Process:** The organisation will provide clear instructions and assistance to guest account holders to ensure the enrolment of MFA methods. This may include guidelines, training, and support to set up MFA.

5. **Exemptions:** Exemptions from this policy may be considered on a case-by-case basis with a valid business justification. Requests for exemptions should be submitted to the IT department for review and approval.

6. **Monitoring and Enforcement:** The IT department will regularly monitor compliance with this policy and take appropriate actions to enforce it. Non-compliance may result in account suspension or revocation.

7. **Policy Review:** This policy will be reviewed periodically, at least annually, to ensure its effectiveness and relevance. Any necessary updates or changes will be made to address evolving security threats and technology.

8. **Implementation:** This policy will be implemented by the IT department in collaboration with the relevant stakeholders. Guest account holders and their sponsors will be notified of this policy, and the IT department will provide support and guidance for MFA setup.

9. **Effective Date:** This policy will be effective as of 20 October 2023, and all existing guest accounts will be required to have MFA enabled within 6 months.

10. **Review Date:** This policy will be reviewed and, if necessary, updated in conjunction with the usual policy review cycle.