Cybersecurity Policy

Entity:	Integrity Financial Planners Pty Ltd **(IFP)**
ABN:	71 069 537 855
AFSL:	225051

Template Administration History – Version Controls			
Action (e.g. creation)	**Date**	**Version Number**	**Description/Reason (e.g. new precedent)**
Creation	01/06/2023	1.0	New policy

Contents

Intellectual Property and disclaimer

This document was originally created in August 2023 by Integrity Financial Planners Pty Ltd (IFP). All present and future rights to intellectual property in this document shall remain with IFP. While IFP endeavours to ensure the accuracy of this document, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this document.

Version 1.0 – August 2023

References:

1. **Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs):** The Privacy Act and APPs regulate the handling of personal information, including client data. Financial planners are required to implement measures to protect the confidentiality and security of client information and report any data breaches promptly.

2. **ASIC Regulatory Guide 104 (RG 104) - Licensing: Meeting the General Obligations:** This guide outlines the general obligations for financial services licensees, which includes implementing adequate cybersecurity measures to protect client information and systems.

3. **ASIC Cyber Resilience Good Practice Guide (RG 281):** This guide provides recommendations and best practices for enhancing cyber resilience in the financial services industry. Financial planners are encouraged to follow these guidelines to protect against cyber threats.

4. **Financial Sector (Business Continuity Management) Guidance Note (ASIC GN 232):** This guidance note outlines the expectations for business continuity management in the financial sector, which includes cybersecurity incident response and recovery plans.

5. **Corporations Act 2001 (Cth):** While not explicitly focused on cybersecurity, the Corporations Act requires financial planners to act in the best interests of their clients and provide suitable advice. Implementing robust cybersecurity measures is essential to ensure client data is protected from breaches and misuse.

6. **Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act):** Financial planners are required to conduct customer due diligence and report suspicious transactions, which may involve cybersecurity-related activities.

7. **Notifiable Data Breaches (NDB) Scheme:** Under this scheme, organizations, including financial planners, are required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) in the event of eligible data breaches.

8. **Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234 - Information Security:** While primarily applicable to APRA-regulated entities, this standard sets out cybersecurity requirements that may influence broader industry practices.

It is essential for financial planners to stay updated on any changes or additional legislative requirements that may be introduced over time to ensure they remain compliant with cybersecurity regulations.

1 Background and purpose of document

1.1 Background

(a) Under s912A(1) of the Corporations Act (**Act**), an Australian financial services Licensee (**AFSL**) is required to (amongst other requirements):

(i) do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly;

(ii) comply with the financial services laws;

(iii) take reasonable steps to ensure that its representatives comply with the financial services laws;

(iv) ensure that its representatives are adequately trained and are competent, to provide those financial services; and

(v) comply with the conditions on the licence.

(b) An AFSL must also take reasonable steps to ensure that its representatives comply with Cybersecurity expectations and legislation.

1.2 Purpose and framework

This policy document outlines the cybersecurity guidelines and best practices for IFP as an Australian Financial Services Licensee (AFSL) to adhere to Corporations Act 2001, ASIC's Cyber Resilience Good Practices and the NIST Cybersecurity Framework. The policy aims to provide practical requirements and measures for financial advisers to protect sensitive data, ensure secure communication, and mitigate cyber threats effectively.

1.3 Scope

This policy applies to all IFP and their employees; Corporate Authorised Representatives (CAR) and their employees; Sub Authorised Representatives (SAR); contractors; and third-party service providers associated with the Corporate Authorised Representatives and / or IFP. It covers all digital assets, systems, and data managed or accessed by IFP and their CARs and SARs, irrespective of their location.

2 Responsibilities

2.1 IFP Management

A Responsible Manager (or a delegate with appropriate experience and seniority) will be responsible for:

(a) Establishing a cybersecurity management framework that aligns with *Corporations Act 2001,* ASIC Cyber Resilience Good Practices and the NIST Cybersecurity Framework;

(b) ensuring that the representatives understand the requirements of this Policy;

(c) monitoring compliance with this Policy via its Monitoring and supervision policy; and

(d) reviewing this Policy on not less than an annual basis (unless more immediate updates are required due to legislative or regulatory change);

(e) undergoing regular cybersecurity awareness training to understand and mitigate potential risks;

(f) report and manage any suspicious activities or potential security breaches immediately to the designated authority;

(g) review the need for Cybersecurity insurance across the AFSL.

2.2 CARs

All CARs appointed under IFP are responsible for:

(a) Familiarising themselves with this policy and complying with its guidelines;

(b) Establishing a cybersecurity management policy and framework within their business that aligns with this policy, along with a risk assessment and response plan;

(c) Designating a Chief Information Security Officer (CISO) responsible for overseeing cybersecurity operations and incident response (this may be an external resource);

(d) Ensuring all employees and contractors who deal with sensitive client information undergo regular cybersecurity awareness training to understand and mitigate potential risks;

(e) Reviewing contracts with external resources to ensure a high level of cybersecurity is applied by the contractor/s;

(f) Reporting any suspicious activities or potential security breaches immediately IFP

2.3 SARs and CAR employees

All SARs and employees of CARs are responsible for:

(a) Familiarising themselves with this policy and complying with its guidelines;

(b) Undergo regular cybersecurity awareness training to understand and mitigate potential risks;

(c) Report any suspicious activities or potential breaches immediately to the designated authority.

3 Risk Assessment and Management

3.1 Risk Assessment

(a) Conduct regular risk assessments to identify and evaluate cybersecurity risks to the AFSL, using a risk-based approach.

(b) Prioritize identified risks based on their potential impact and likelihood of occurrence.

3.2 Risk Management

(a) Develop and implement risk management strategies to address identified cybersecurity risks effectively.

(b) Continuously assess and review risk mitigation measures to ensure their ongoing effectiveness.

4 Access Controls

4.1 Identity and Access Management:

(a) Implement strong authentication mechanisms, such as multi-factor authentication (MFA), for systems and applications containing sensitive information.

(b) Assign access rights based on the principle of least privilege to limit access to data and systems to only those who require it for their job responsibilities.

4.2 Employee Onboarding and Offboarding:

(a) Establish a process for granting and revoking access to systems and data during employee onboarding and offboarding.

(b) Conduct periodic access reviews to ensure that access privileges are up to date and aligned with employees' current roles.

5 Australian Signals Directorate (ASD) Essential Eight

It is a requirement of each practice within IFP to implement and maintain secure configurations for all hardware, software, and network devices, following the ASD Essential Eight guidelines.

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the *Strategies to Mitigate Cyber Security Incidents*, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks. While the principles behind the Essential Eight may be applied to cloud services and enterprise mobility, or other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate to mitigate unique cyber threats to these environments.

The mitigation strategies that constitute the Essential Eight are:

- application control
- patch applications
- configure Microsoft Office macro settings
- user application hardening
- restrict administrative privileges
- patch operating systems
- multi-factor authentication
- regular backups.

Implementing the Essential Eight

The Essential Eight Maturity Model articulates requirements for the implementation of the Essential Eight.

Assessing implementations of the Essential Eight

Assessments against the Essential Eight should be conducted using the Essential Eight Assessment Process Guide.

Further information

Further information on the Essential Eight Maturity Model and its implementation is available in the Essential Eight Maturity Model FAQ publication https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-faq

6 Patch Management

Establish a process for timely and regular application of security patches to mitigate known vulnerabilities, following the ASD Essential Eight guidelines.

7 Network Security

Implement strong network security measures, including firewalls, intrusion detection/prevention systems, and secure remote access controls, following the ASD Essential Eight guidelines.

8 Data Protection and Encryption

Implement encryption mechanisms for sensitive data, both in transit and at rest, to prevent unauthorized access or data breaches, following the ASD Essential Eight guidelines.

9 Security Awareness and Training

Conduct regular cybersecurity awareness and training programs for all employees and advisers to educate them about potential threats, social engineering attacks, and safe cybersecurity practices.

10 Incident Response and Reporting

10.1 Incident Response Plan:

(a) Develop and maintain an incident response plan that outlines the steps to be taken in case of a cybersecurity incident or breach.

(b) Test the incident response plan periodically through simulations and tabletop exercises.

The ASD has released a Cyber Security Incident Response Plan ACSC Emergency Response Guide (cyber.gov.au) which provides guidance on how to put together your Cyber Incident Response Plan. IFP recommends that each CAR under its AFSL adopts this Cyber Incident Response Plan and completes each of the templates, tailored to their practice, covering the following:

Appendix B – Cyber Security Incident Response Readiness Checklist

Appendix C – ASD cyber security incident triage questions

Appendix D – Situation Report Template

Appendix E – Cyber Security Incident Log Template

Appendix F – Evidence Register Template

Appendix G – Remediation Action Plan Template

Appendix H – Post Cyber Security Incident reviews

Appendix I – Action Register Template

A template of the "Cyber Security Incident Response Plan" can be found at www.iplan.com.au.

10.2 Incident Reporting:

(a) Establish clear procedures for reporting cybersecurity incidents to the appropriate authorities within the AFSL.

(b) Comply with regulatory requirements for reporting cybersecurity incidents to ASIC or other relevant authorities.

11 Data Protection and Encryption

Implement encryption mechanisms for sensitive data, both in transit and at rest, to prevent unauthorized access or data breaches.

12 Third-party Risk Management

(a) Evaluate and assess the cybersecurity practices of third-party service providers and vendors who have access to the AFSL's data or systems.

(b) Establish contractual agreements that include cybersecurity requirements and responsibilities for third-party vendors.

13 Monitoring and Continuous Improvement

(a) Implement security monitoring tools and practices to detect and respond to cybersecurity threats in real-time.

(b) Continuously review and improve cybersecurity practices based on emerging threats and lessons learned from security incidents.

14 Compliance and Audit

(a) Regularly conduct internal cybersecurity audits to ensure compliance with this policy, ASIC Cyber Resilience Good Practices, and the NIST Cybersecurity Framework.

(b) Address any non-compliance issues promptly and implement corrective actions.

15 What do you need to do?

As Cyber Security has typically been an element addressed in IT security, it is very likely that your IT expert / firm has a plan regarding the protection of your client data and a plan for what to do if your client data is compromised.

It is imperative that the Director/s of your CAR and all staff are aware of Cyber risks and what to do in the instance that a cyber attack occurs or is attempted, whether that be a spam email or a ransom attack.

As noted previously in this Policy, the ASD has released a Cyber Security Incident Response Plan. Your first action should be to review this document; complete the templates; prepare your Playbooks and then to complete ongoing training.

Should you require any assistance with putting together your Cyber Security collateral, please contact IFP.

16 Consequences

The responsibility for ensuring CyberSecurity measures are appropriate, effective and meets the ASIC requirements, lies with the Director/s of each Corporate Authorised Representative (CAR) of IFP.

There are very heavy fines and consequences to the Director/s and then the AFSL if CyberSecurity measures are not adequate in assisting to protect client data from cyber attacks. As per the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022,* the maximum penalties for serious or repeated privacy breaches increased from $2.22 million to whichever is the greater of:

- $50 million;
- Three times the value of any benefit obtained through the misuse of information; or
- 30% of a company’s adjusted turnover in the relevant period.

17 Conclusion

This cybersecurity policy is designed to protect the AFSL, CARs, financial advisers, and clients from cyber threats by adhering to best practices recommended by ASIC and NIST. Regular review, updates, and cooperation from all stakeholders are essential to ensure the policy's ongoing effectiveness in mitigating cyber risks and maintaining a secure environment for financial services operations within Australia.