LCollect

Collection Law Partners

BH Lawyers

APRA Compliance Information Security

Prudential Standard CPS 234

first edition

CONTENTS

Introduction

The Australian prudential Regulation Authority (APRA) Prudential Standard CPS 234 (CPS 234) requires APRA-regulated entities and third-party providers to develop and maintain robust and secure information Security Infrastructure, Policies and Procedures. Due to the sensitive and personally identifiable data that LCollect Pty Ltd and BH Lawyer Pty Ltd (incorporating Collection Law Partners), herein "**the Group**", utilise in their daily business operations; it is recognised that this is the minimum requirement to ensure that any potential data exposure is minimised.

Under CPS 234 it is expected that an entity understands 3 key factors, the threat landscape, risk associated with the business based on the sensitivity of data and propensity as a target, and cybersecurity maturity as a business. The Group have undertaken a full risk assessment with the understanding that our data was high-risk and our cyber security maturity was also high. Based on the risk vs maturity as outlined by the federal Government, in order to fully comply with APRA requirements, our security posture needed more structure and coordination.

Roles & Responsibilities

The board of an APRA-regulated entity is ultimately responsible for information security. The board must ensure the entity maintains information security in a manner reflective of its size and extent of threats to its information assets and enables the continued sound operation of the entity.

The Group have tasked their executive to oversee the end-to-end security of our data. The executive will act as the board for the purpose of monitoring and assessing APRA standards and requirements. As an SME the Executive are hands on and are best positioned to control the ISMS and ensure data integrity and compliance.

Information Security Capability

An APRA-regulated entity must have information security capability which corresponds with the size and threats to its information assets and enables the continued sound operation of the entity.

As an SME group, the Group have assessed their information usage, Data protection requirements and security infrastructure and believe we have a superior security posture to most businesses of a like size. We have a mix of hardware and application-based security services that are ISO27001 compliant and give us this level confidence.

Creating an Information Security Policy Framework

An information security policy framework must be maintained and provide direction on responsible parties who have an obligation to maintain information security.

The Group have developed a comprehensive security policy framework that covers all areas of APRA CPS234 and PCI DSS requirements. The policy covers all necessary aspects from Authority and Delegation, job function data requirements, Physical and logical security, data storage, security and back up requirements. It also outlined recruitment and required background checks, compliances required and testing and reporting.

Information Asset Identification & Classification

Information assets must be classified based on criticality and sensitivity. These classifications must reflect the potential impact of an information security incident on the entity and the interests of depositors, policyholders, beneficiaries and customers.

All assets used in the company are categorised based on data access and storage requirements, environment and risk. Where possible we utilise ISO27001 compliant cloud environments that comply with CPS 231 and Data Protection Regulations. Our Cloud instances are secured using secure VPN for access and Cloud intrusion monitoring services.

Implementation of Controls

Controls must be in place to protect information assets including those managed by a related or third party.

The Group are in the process of auditing all suppliers to ensure compliance with Essential 8 Security practices. This is the minimum requirement for data and IT security as outlined by the ACSC (The Signals Directorate). Any contractors that must utilise sensitive or personally identifiable data are vetted to ensure compliance with data protection requirements and legislation. Contracts are being modified to incorporate cyber security as a necessity.

Testing of Control Effectiveness

A systematic testing program must be implemented to test the effectiveness of information security controls. These controls must be tested and conducted by skilled, independent specialists at least annually.

The Group have completed the initial Internal and External Penetration Testing and have implemented improvements and recommendations associated with the findings. This was completed first week of 2021. The testing found that our security infrastructure (Firewall, Malware detection and Interception and email and web security services) linked well to secure our environment.

Areas of improvement were based on password policy that has now been hardened as per recommendations and some applications needed the latest patching. This is all completed.

Incident Management

Robust mechanisms must be in place to detect and respond to information security incidents. These mechanisms must manage all relevant stages of an incident, from detection to post-incident review as well as escalation and reporting of incidents to the boards, governing bodies and individuals responsible for the management of security incidents.

As part of the risk assessment, policies are in place to ensure incident management is structured and coordinated. Procedures have been documented and disseminated, authorities have been established and escalations have been outlined. The board will oversee any action plan resulting from an incident and all required reporting.

Auditing

Audit of the information security controls must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties.

As an SME our auditing is incorporated in our risk analysis exercises. We are developing a full ISMS that will be APRA compliant with a view to expanding this to ISO27001 compliance. This will be audited as per the ISO27001 standards requirement utilising specialist external independent companies / contractors.

Notifying APRA

APRA regulated entities must notify APRA as soon as possible (and no later than 72 hours) after becoming aware of an information security incident that has materially affected or has the potential to affect materially, financially or non-financially, the entity or the interest of depositors, policyholders, beneficiaries or other customers. Notification must also occur if an incident has been notified to other regulators, either in Australia or other jurisdictions.

If an information security control weakness is identified, the entity must notify APRA as soon as possible or no later than ten business days after it becomes aware of the weakness.

The Information Security Policy sets out the process to ensure incident and vulnerability reporting is an integral part of the security process. As this policy is overseen by the board, the reporting requirements are native to the policy and adherence is assured.