RIMPA

GLOBAL

Status Upgrade Sample Responses

31.08.23

RECORDS AND INFORMATION MANAGEMENT PRACTITIONERS ALLIANCE

Advancing and Connecting the Records and Information Management Profession

ASSOCIATE MEMBER – INFORMATION SECURITY

UNDERSTANDS INFORMATION SECURITY NEEDS, REGULATORY REQUIREMENTS AND FRAMEWORKS.

I understand that information needs to be protected to minimise the risk of unauthorised or inappropriate access, use, disclosure, deletion, destruction and tampering. The three elements that need to be considered are confidentiality, integrity and availability. Effectively managing the security of information reduces risk and means that agency information is: Disclosed or released appropriately; Trusted and able to be relied upon; Available when needed. In our agency information security is governed by [list artefacts] …

IS ABLE TO IMPLEMENT RELEVANT CONTROLS AND PROCEDURES, AND CONDUCT INFORMATION SECURITY RISK ASSESSMENTS AND AUDITS.

In our agency information security is governed by Information Security Standards, Privacy Legislation and our internal Information Security Policy and Classification scheme. To make implementation easier for our staff we apply our information security classifications at the system level through default access controls and security groups in various systems. Our users can change these settings if different security is required. Protecting our digital information in this way is fairly straightforward and easy to control. We also have specific procedures that describe what staff need to do to ensure the same protections are applied to information in physical formats. Each year a security audit is conducted. The focus this year was on information in physical formats. After my manager collects and analyses the audit data we work together to develop a program to educate the staff in how to improve their information security practices. I am involved in developing and delivering some of the information sessions.

CHARTERED MEMBER – INFORMATION SECURITY

IS ABLE TO INTERPRET REGULATORY REQUIREMENTS AND INFORMATION SECURITY POLICY TO ENSURE INFORMATION MANAGEMENT POLICIES AND PROCEDURES ARE ALIGNED TO MEET REGULATORY REQUIREMENTS AND FRAMEWORKS.

I understand that information needs to be protected to minimise the risk of unauthorised or inappropriate access, use, disclosure, deletion, destruction and tampering. The three elements that need to be considered are confidentiality, integrity and availability. In my workplace I have written an information security classification scheme which is based on the Protective Security Policy Framework (the Framework) and the Australian Government Information Security Manual. The Framework has two levels which aren’t relevant to my workplace so I needed to educate my Executive Leadership Team (ELT) about this. Also, the ELT wanted to change the name of two of the classification terms (not how the levels operated just what they were called). In doing this I had to make sure that everyone was clear about the use of the new terms and what types of information to which they were applied and how the security practices would look for each business unit. I am pleased to say our workplace information security framework is now approved and being implemented by all teams.

IS ABLE TO MANAGE INFORMATION SECURITY RISK ASSESSMENTS AND AUDITS, AND COMMUNICATE OUTCOMES AND ISSUES TO BUSINESS MANAGERS AND OTHERS.

Each year I undertake an information security audit to make sure our information security policies are understood and being consistently implemented. The focus this year was on information in physical formats. I have attached the questions for the audit and the results [attach artefacts or links if permitted]. Once the audits are completed I collate the results and display them in a table showing a comparison between the previous audit and this one. I then provide recommendations for areas in which improvement needed to be made. I have attached a de-identified report and recommendation [attach artefacts or links if permitted]. After discussion these with the teams concerned and being accepted by the managers I provide a report for the Executive team and an implementation plan. The Plan is currently being implemented and is expected to be completed by later this year.

FELLOW MEMBER – INFORMATION SECURITY

UNDERSTANDS INFORMATION SECURITY NEEDS AND HOW THEY RELATE TO INFORMATION MANAGEMENT PROCESSES AND ENSURES APPROPRIATE RESOURCES ARE ALLOCATED TO MITIGATE INFORMATION SECURITY THREATS.

I understand and work collaboratively across my organisation to make sure that information security risks are managed. My agency works in a secure environment and we managed some highly confidential information about children. It is very important to maintain the confidentially of this information which is shared on a ‘needs to know; basis even within our organisation. Staff who have access to this information had additional policy checking undertaken to ensure that our information is not inadvertently at risk. I work closely with my IT area to ensure that the systems in which this information is stored are also protected. Apart from the usual internal access audits my IT also ensures that this particular system is not at risk due to cyber-attack or if vulnerabilities are identified they are quickly remediated. Due to the sensitivity of our information I am also on the Data Breach Response Team and play an active role in education and awareness of all staff to make sure they are aware of the many ways in which data breaches may occur and how to respond appropriately. This also includes education about how best to manage our information in physical formats and the importance of clean desks and secure storage. I have attached a sample of a recent awareness talk I provided to a key business area. [attach artefacts or links if permitted]. We have a variety of information sharing obligations with other agencies that also manage the welfare and protection of children. To ensure confidentiality and integrity of shared information we have very specific processes in place to manage risks during the exchange of information. During an Amber Alert (that is the urgent broadcast of information through the media and other means to the public to facilitate the safe recovery of an abducted child) we have an specific information security model to enable information to be quickly and easily shared between agencies until the child is recovered. This is because the risk to the child is considered far greater than the information security risks. That said, there is a detailed agreement that specifies what information is shared, with which agencies and how the sharing will happen securely. This does mitigate much of the information security risks. Immediately after the child is recovered our temporary information security model is revered back to the business-as-usual framework.