icare™ | Insurance for NSW

Useful Tips - Your Cyber Declaration Form

icare | Insurance for NSW

Useful Tips – Cyber Declaration Form

The TMF Statement of Cover provides support to TMF Agencies for their insurable risks arising from Cyber exposures.

In the last few years, the emerging risk known generally as Cyber has become an issue for all organisations worldwide, Government agencies are vulnerable to cyber-attacks and this has been heightened with the change in working practices. TMF has responded by confirming to agencies that their insurable risk arising from Cyber exposures is supported within the TMF Statement of Cover. Cyber incidents have risen in the last two years and we are keen to get a better understanding of the exposure, and importantly, the risk management practices. To understand risk factors and account for resulting exposures, we need to ask questions surrounding this relatively new TMF contribution assessment factor.

From our thorough review of previous cyber declaration data declared by our Agencies, we identified several areas where information declared was not consistent or common mistakes were made. icare has liaised with Cyber NSW and our cyber security specialist to review the questions this year, we have added questions around emerging exposures, contracting with vendors and third parties that have access to your agency data, where that third party has a cyber event and as a consequence, your data which they hold is also compromised.

We've developed this useful tip sheet to assist you in completing your Cyber Declaration Form. Please enter responses for all questions as well as additional details when requested in the text response field. The question set should reduce in future years as our partners gain a greater understanding of agency network controls.

Sections

The Cyber Declaration Form has been separated so that it can be directed to your agency's Business Technology Leads, who will provide information around how your information is stored and protected. The form has been split into three sections:

1. Cyber Liability
2. Cyber Enterprise Risk Management
3. Personal Records.

Always Save a Copy of Your Work

1. It is recommended that **PDF copies** of all sections and forms **are retained by each Delegate and Coordinator prior to submitting** information for final approval.
2. When using the Download PDF button, Delegates will receive a PDF of the specific section of the form which they have completed.

3. 'Download PDF' will generate the contents of the entire Declaration Form, including all the Sections within it, as a PDF document.
4. If you are attaching any file to your TMF Declaration, please keep a copy. This includes the Excel spreadsheets that have been generated from the Ventiv system.

Some words and explanations used in the Cyber Declaration

Some words and explanations used in the Cyber Declaration

Passwords	Poor password control is a key entry point for threat actors. Diligent password control should be a key network hygiene point and system protection tool for information system controllers.
Network Access	Human error and rogue employees contribute to approximately 25% of all cyber claims. One way of limiting the impact of incidents coming from these areas is to limit system access for staff to their area of role responsibility. Capture the practices applied to remove or disable access from staff once they have resigned or changed job functions.
Network Segmentation	Network segregation / segmentation helps reduce the ability of malware or intrusion spreading through a network. It is like having fire doors in a building. Basic computer hygiene should include limitation on network access to areas required for specific job function as opposed to a person title. Confirm if your agency implements network segmentation between critical and non-critical areas.
Network Protection Basics	Patch management is one on the ASD's (Australian Signal Directorates) recommended mitigating strategies against cyber events. Find more information: https://www.asd.gov.au/infosec/mitigationstrategies.htm https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm
	Application White listing - A whitelist only allows selected software applications to run on computers. Why? All other software applications are stopped, including malware.
	Disable untrusted Microsoft office macros - Microsoft Office applications can use software known as 'macros' to automate routine tasks. Why? Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled.
	User Application Hardening - Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet. Why? Flash, Java and web ads have long been popular ways to deliver malware to infect computers.
	Patch Application - A patch fixes security vulnerabilities in software applications. Why? Adversaries will use known security vulnerabilities to target computers.
System Backup	With the rise of ransomware as an attack tool by threat actors, secure and regular backup of information systems and data is becoming a key component to help defeat this malicious software. There should be a control mechanism checking backups for completion and checks for any file corruption so that it supports the ability to call up files when needed. Describe how often your agency backs up your information systems.
Network Traffic	It is important to be aware of what normal network traffic looks like in order to assist in being able to spot unusual network activity. Unusual activity could be a sign of network infection that should be investigated internally. Describe how and how often your agency monitors network traffic.
Intrusion Detection	Intrusion Detection Systems act as a type of Burglar Alarm on your network that will detect an intruder or attack and issue some type of warning. Explain if your agency has this type of software installed to safeguard your network.

Outsourcing IT	If your agency outsources any if it's IT services, identify the areas of operation.
Encryption	Encryption protects data from prying eyes. Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it. Describe how your agency encrypts personal or back-up data.
Industrial Control Systems & SCADA	Control systems apply to the systems that control, monitor and manage large production systems.

1. Cyber Liability Section

Provide a yes/no response and/or additional information as requested.

Network Access: Human error and rogue employees contribute to approximately 25% of all cyber claims. One way of limiting the impact of incidents coming from these areas is to limit system access to their area of role responsibility.

- Please describe the process implemented by your agency to remove or disable network access from staff after they have resigned or changed job function.
- Please specify whether your agency provides network access to staff based on job function or a staff position.

Network segmentation/segregation: Helps reduce the ability of malware or intrusion spreading through a network. It is like having fire doors in a building. Basic computer hygiene should include limitation on network access to areas required for specific job function as opposed to a person title. To answer the Segmentation question, you will need to know if you have multiple segments / sub-nets, allowing more control over data flow and security and whether you validate the architecture is segmented to limit risk as appropriate.

- Does your agency implement network segmentation to separate critical areas from non-critical areas? *Yes/No and details requested.*

Personal information: The intent of this question is to understand the level of agency compliance with personal information access and internal processing controls. Does segmentation allow privacy and security for authorised persons only, in respect of personal information (financial, health, other details), or critical industrial equipment operating systems, such as water, powerplants, sewage pumping stations and the like?

- Does your agency implement cyber security awareness training across all staff and contractors at least annually, including those authorised to access or process personal data? *Yes/No and details requested. For example, do you have mandatory formal data privacy and cyber security training required for staff, including contractors and is this logged against the individuals training record?*

Network Protection Basics: Patch management is one of the ASD's (Australian Signal Directorates) recommended mitigating strategies against cyber events. Operating systems of devices are commonly exploited and as a result security patches are always being developed / updated to protect data. All updates should be maintained to ensure security is up to date.

- Does your agency update all system security patches and antivirus regularly? *Yes/No and details requested*

System Backup: With the rise of ransomware as an attack tool by threat actors, secure and regular backup of information systems and data is becoming a key component to help defeat this malicious software. There should be a control mechanism checking backups for completion and checks for any file corruption so that it supports the ability to call up files when needed.

- Does your agency backup and check network information regularly? *Yes/No and details requested. If yes, provide details of testing of back-ups and how often these are undertaken.*
- If yes, please confirm if back-ups are stored at off-site locations.

It's important to have good data backed up in a safe place, due to attacks with malicious software, designed to intrude in order to steal, or damage data. It's also important to periodically restore backed up data to ensure the data is intact and useable. This should be performed by authorised persons only.

Network monitoring: It is important to be aware of what normal traffic looks like in order to be able to assist in being able to spot unusual network activity. Unusual activity could be a sign of network infection that should be investigated internally.

- Is your network traffic regularly monitored? Yes/No and details requested

Network monitoring tools are available commercially, as well as the technology team monitoring the system data movement to ensure large data is not moving without appropriate authority, or suspicious emails and web portal access are intercepted.

Intrusion systems: Most likely a third party software and IT staff managing any suspicious, or known virus, malware, ransomware, unauthorised access intrusions.

- Is an intrusion detection system implemented? Yes/No and details requested.
- Please list your agency's preferred provider of outsourced IT services, identify each provider's area of operation and list the intrusion software used.

Encryption: Encryption protects data by changing data to ciphertext, which protects data from prying eyes. Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it.

- Does your agency encrypt all personal data stored upon your information systems? Yes/No. If no, details are requested in relation to any other measures to protect personal data.
- Are backups containing personal data also encrypted? Yes/No. If yes, details requested. If no, details are requested in relation to any other measures to protect personal data.
- Personal data is encrypted when transmitted over the network. Yes/No
- Mobile devices and laptop hard disks are encrypted. Yes/No
- Has your agency sustained any loss of revenue from network usage due to a cyber event, distributed denial of service, tampering, infection with malicious code or other type of cyber-attack? If yes, details regarding loss of revenue are requested.

SCADA: Supervisory Control and Data Acquisition used to collect and control industrial processes from a remote location, such as pumps, sensors, valves, electric motors and the like.

- Does your agency use or is responsible for the operation of any Industrial Control Systems / SCADA systems? Yes/No.
- . If no, further details are requested. If yes, 2 further questions requesting further details regarding connection of the systems to the internet and whether passwords of these systems are changed from any default settings

Essential 8: For the 'Essential 8' strategy, please see following link: *https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model*

- Has your Agency adopted the key controls for strategies to mitigate and prevent cyber incidents, as per the Australian Cyber Security Strategy Essential 8? Yes/No. If yes, choose the Agency's level of maturity between 0-3.
- Does your Agency include cyber security in the Risk Management framework? Yes/No

Contracting with vendors, suppliers and partners who have access to internal agency or agency customer data, systems, processes or other privileged information

- Do you review that Vendor/supplier/partner's system security has been tested for vulnerabilities during on-boarding? Yes/No. If yes, provide commentary on how this is managed. If no, have you received a recent report with security testing results?
- Do you check Vendor/supplier/partner's own staff cyber awareness programmes/training? Yes/No and additional comments are requested.
- Do you have a Vendor cyber security policy? Yes/No. If yes, provide details
- Do you check that the Vendor has current and adequate cyber insurance in place which includes loss to third parties? Yes/No and additional comments are requested

Always obtain a Certificate of Insurance from vendors showing limits of cover and any "Excess" or franchise, refer to fee payable when lodging a claim. Refer to the *Contractual Liability – Risk Management Bulletin* for guidance on adequate cyber insurance cover.

2. Cyber Enterprise Risk Management Section

Provide a yes/no response to the following questions, only the cyber management plan requires additional information.

Cyber Management Plan

- Do you have a current cyber response plan in place, which links into the agency incident response plan (Business Continuity Plan)?
- If yes, a comments field is provided for further information regarding whether this plan has been tested by a real or mock cyber event.

Information Security (IS)

- You identify critical information systems risks and implement appropriate controls to mitigate them
- Regular audits of the IS are conducted and resulting recommendations are prioritised and implemented

- Information resources are inventoried and classified according to their criticality and sensitivity

Information Systems Protection

- Access to critical information systems requires dual authentication

Network Security and Operations

- Penetration testing is conducted regularly and a remediation plan is implemented where necessary
- Vulnerability assessments are conducted regularly and a remediation plan is implemented where necessary
- Procedures for incident management and change management are implemented
- Security events such as virus detection, access attempts, etc…, are logged and monitored regularly –

Physical Security of Computing Room

- Critical systems are duplicated according to Active/Passive or Active/Active architecture
- Critical systems are duplicated on two separate premises

Outsourcing

- You have not waived your rights of recourse against the products / service provider in the outsourcing contract

3. Personal Records Section

This entails a few questions to understand the nature and volume of personal records held by the agency. Most agencies handle large numbers of personal and/or confidential information.
Given the increase in cyber-attacks in recent times, a hacker could potentially access any of the databases and the personal records held, if care was not taken to protect data. As a result, we need to understand the potential risk exposure of data stored and used which could be affected if the Agency's systems were breached and information stolen, damaged or accessed and copied, and taking account of risk exposure and damage to people trusting government with sensitive personal data.

The important thing is not number of records but number of persons affected. E.g. Number of patient records held by each hospital etc. This includes current and historic (1 patient = 1 record), number of employee records held by each Agency (1 employee = 1 record).

We are not after absolutely accurate numbers, but best estimate that the Agency can provide for the 3 types of personal records.

Personal record means any item, collection, or grouping of information about an individual that is maintained by an agency. It includes, but is not limited to, the individual's:

- Education
- Financial
- Medical
- Employment history
- Items that contain or make reference to the individual's name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

We consider HR databases to be personal records.

A **personal health record (PHR)** refers to the collection of an individual's medical documentation. This includes details such as but is not limited to:

- The patient's medical history
- Applicable diagnoses
- Historical and ongoing medications, including over-the-counter and alternative treatments
- Past medical and surgical interventions
- Immunization status
- Allergies and other relevant medical conditions that can impact the delivery of emergency care
- Blood type
- Whom to contact in the event of an emergency
- Insurance information
- Contact information for the patient's regular health providers
    - Select the types of personal records held. For each type of record held, you must enter the maximum number of records held:
    - PII - Personal Information (Emails, DOB, names and addresses, usernames and passwords)
    - PCI - Personal records containing credit card information (payment card information - credit/debit cards, banking and other financial information)
    - PHR - Personal medical and health records (refers to the collection of an individual's medical documentation)

Provide the best estimate of the number of records held over the 12-month declaring period in each category. Add zero (0) if no personal records are held for the relevant category.

The system will calculate the total number of records held across those 3 types. You are also given the opportunity of providing additional information to qualify your response.

If you require further assistance with this, please contact your icare Client Engagement Manager or email declarations@icare.nsw.gov.au.