Cyber Security Questionnaire / Declaration

Overview

In accordance with Protective Security Policy Framework (PSPF) Direction 001-2024-managing Foreign Ownership, control and Influence, Services Australia requires all suppliers of hardware, software and cloud services to undergo a cyber security assessment.

The purpose of this business Cyber Security Questionnaire is to provide the agency with detailed information to assess supply chain risk against the agency's ICT environment.

Instructions

This questionnaire covers a broad range of cyber security topics including Foreign Ownership, Control or Influence (FOCI), Security Practices, Transparency and Data Sovereignty.

Elements of the questionnaire will require business involvement and possibly the re-seller. While multiple parties may be involved to answer some sections, the agency requests the business signatory to sign the declaration.

Please complete all questions on this form. Mark 'Yes' or 'No' for each question. For answers of 'Yes', please provide details in the 'Supporting Comments' area to complete the answer.

Only completed forms will be accepted.

Information obtained will be held in confidence and in accordance with legislative requirements (e.g. Privacy Act 1988 and Freedom of Information Act 1982). In some cases, information may be passed to third parties (e.g. Australian Security Investments Commission) for verification purposes only.

The terms "foreign person(s") and "foreign corporation" has the interpretations given in the Foreign Acquisitions and Takeovers Act 1975.

Please note:

- All questions must be answered.
- Where appropriate provide as much information as possible to support your answer.
- Where you have answered 'yes' to a question, evidence must be available at the agency's request.
- Where you have answered 'no' or 'unsure', please provide a brief explanation as to why this is the case.
- Assessment of a Business suitability will be made on the information provided in this questionnaire. Please ensure your responses are true and correct to the best of your knowledge.

Definitions	
Business	Distributor, Supplier, Manufacturer (OEM), Retailer
Re-seller	Third Party Provider/Supplier
Product/Service	Hardware, Software, Cloud Services

Business Details		
#	Question	Business Answer
1	Entity legal/trading name	
2	Registered ABN	
3	Registered Address	
4	Product/Service Name	
5	If applicable, RFQ Number	

Business Details			
#	Question	Business Answer	
Foreign Ownership, Control or Influence (FOCI)			
1	Where is the business headquartered?		
2	Where does the business operate from?		
3	What are the nationalities of board members and employees?		
4	Who has controlling shares in the business?		
5	Is the business profitable or financially stable?		
6	Does the business use sub-contractors for any of the product or service lifecycle stages e.g. design, development, manufacturing, distribution, maintenance or disposal?		
Security Practices		**Business Answer**	**Supporting Comments**
7	Has the business made a commitment to secure-by-design practices for their products and services?	Yes/No	remarks
8	Does the business have a vulnerability disclosure policy?	Yes/No	
9	Does the business have a mandatory cyber security incident disclosure policy?	Yes/No	
10	Does the business have a mature Cyber Security Risk Management Program?	Yes/No	
11	If applicable, has the business provided a Software Bill of Materials (SBOM)? If yes, please provide documentation.	Yes/No	

12	If applicable, has the business provided a Hardware Bill of Materials (HBOM)? If yes, please provide documentation.	Yes/No	
13	Does the business follow a cyber security standard for their own system? e.g. NIST, ISO 27001, ISM, Essential 8	Yes/No	
14	Does the business actively manage risks in their own supply chains (including sub-contractors)?	Yes/No	
15	Has the business' service or product been independently security evaluated and listed on the Common Criteria Certified Product List?	Yes/No https://www.commoncriteriaportal.org/products/index.cfm	
16	Has the business been compromised previously?	Yes/No	
Transparency			
17	Does the business conduct penetration testing regularly (min annually) on their products and services?	Yes/No	
18	Does the business allow externals to conduct penetration testing on the business's products and services?	Yes/No	
19	If applicable, do products and services operate with privileged access?	Yes/No	
20	If applicable, do products and services require enduring access to the internet?	Yes/No	
Data Sovereignty			
21	If applicable, will systems or data be accessed from anywhere other than Australia?	Yes/No	
22	Will data be stored anywhere other than in Australia?	Yes/No	
23	Is the data stored in a HCF certified data centre?	Yes/No	
Business/Re-seller Questions			
24	Does the business conduct background checks on individuals before they re employed?	Yes/No	
25	Does the business and/or re-seller offer anonymity for purchasers if products are sourced from overseas?	Yes/No	

26	Is there any other factor(s) that indicates or demonstrates a capacity on the part of a foreign person(s) or foreign corporations to control or influence the operations or management of your organisation?	Yes/No	

The business signatory is to sign the declaration:

Acknowledgement

☐ I declare that the information provided for the preparation of this activity statement is true and correct.
(INSERT Signature Block here)

The Agency may seek clarification or additional information from you at any time. You must reply in writing to any request from the Agency under this section within 5 working days of that request.

Part X -Seller Response Form - Essential Eight Compliance

Reference Guidelines

Seller Name	
Contact Name	
Contact Role	
Contact Address	
Contact Number	
Contact Email	

#	NAME	ACTION
1	Essential 8 Questionnaire	*Please provide a response in **Column E** titled "Implementation Status" and in **Column F** titled "Implementation Comments" for all rows in ML2:* *- For every cell in **Column E** please describe whether the control is or isn't implemented* *- In **Column F**, where a control is implemented please provide a one to two sentence description of how the control is implemented*

To assist with completing the spreadsheet here are some example responses below. Generally, a sentence for each control is sufficient, noting that some controls may not be applicable for all systems, in which case, N/A is a perfectly acceptable response for implementation status.

Identifier	ML2	Description	Implementation Status	Implementation Comments
ISM-1175	Yes	Privileged user accounts are prevented from accessing the internet, email and web services.	Implemented	Firewall and AD policies prevent administrator access to the internet from management networks and access is blocked for external email and web service access.
ISM-1648	Yes	Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	Partial	Privileged access to systems and applications is strictly controlled and revoked when no longer needed. This is still a manual process for some systems, with migration to the new security platform for the remaining systems scheduled for January 2024

Topic	Identifier	Description	Implementation Status	Implementation Comments
Patch applications	ML2-PA-01	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.		
	ML2-PA-02	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.		
Multi-factor authentication	ML2-MF-01	Multi-factor authentication is used to authenticate privileged users of systems.		
	ML2-MF-02	Multi-factor authentication is used to authenticate unprivileged users of systems.		
	ML2-MF-03	Multi-factor authentication used for authenticating users of online services is phishing-resistant.		
	ML2-MF-04	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.		
	ML2-MF-05	Multi-factor authentication used for authenticating users of systems is phishing-resistant.		
	ML2-MF-06	Successful and unsuccessful multi-factor authentication events are centrally logged.		
	ML2-MF-07	Event logs are protected from unauthorised modification and deletion.		
	ML2-MF-08	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		
	ML2-MF-09	Cyber security events are analysed in a timely manner to identify cyber security incidents.		
	ML2-MF-10	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.		
	ML2-MF-11	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.		

Topic	Identifier	Description	Implementation Status	Implementation Comments
	ML2-MF-12	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.		
Restrict administrative privileges	ML2-RA-01	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.		
	ML2-RA-02	Privileged access to systems and applications is disabled after 45 days of inactivity.		
	ML2-RA-03	Privileged operating environments are not virtualised within unprivileged operating environments.		
	ML2-RA-04	Administrative activities are conducted through jump servers.		
	ML2-RA-05	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.		
	ML2-RA-06	Privileged access events are centrally logged.		
	ML2-RA-07	Privileged account and group management events are centrally logged.		
	ML2-RA-08	Event logs are protected from unauthorised modification and deletion.		
	ML2-RA-09	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		
	ML2-RA-10	Cyber security events are analysed in a timely manner to identify cyber security incidents.		
	ML2-RA-11	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.		
	ML2-RA-12	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.		
	ML2-RA-13	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.		

Topic	Identifier	Description	Implementation Status	Implementation Comments
Application control	ML2-AC-01	Application control is implemented on internet-facing servers.		
	ML2-AC-02	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.		
	ML2-AC-03	Microsoft's recommended application blocklist is implemented.		
	ML2-AC-04	Application control rulesets are validated on an annual or more frequent basis.		
	ML2-AC-05	Allowed and blocked application control events are centrally logged.		
	ML2-AC-06	Event logs are protected from unauthorised modification and deletion.		
	ML2-AC-07	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		
	ML2-AC-08	Cyber security events are analysed in a timely manner to identify cyber security incidents.		
	ML2-AC-09	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.		
	ML2-AC-10	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.		
	ML2-AC-11	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.		
Restrict Microsoft Office macros	ML2-RM-01	Microsoft Office macros are blocked from making Win32 API calls.		
	ML2-AH-01	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		

Topic	Identifier	Description	Implementation Status	Implementation Comments
User application hardening	ML2-AH-02	Microsoft Office is blocked from creating child processes.		
	ML2-AH-03	Microsoft Office is blocked from creating executable content.		
	ML2-AH-04	Microsoft Office is blocked from injecting code into other processes.		
	ML2-AH-05	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.		
	ML2-AH-06	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		
	ML2-AH-07	Office productivity suite security settings cannot be changed by users.		
	ML2-AH-08	PDF software is blocked from creating child processes.		
	ML2-AH-09	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.		
	ML2-AH-10	PDF software security settings cannot be changed by users.		
	ML2-AH-11	PowerShell module logging, script block logging and transcription events are centrally logged.		

Topic	Identifier	Description	Implementation Status	Implementation Comments
	ML2-AH-12	Command line process creation events are centrally logged.		
	ML2-AH-13	Event logs are protected from unauthorised modification and deletion.		
	ML2-AH-14	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		
	ML2-AH-15	Cyber security events are analysed in a timely manner to identify cyber security incidents.		
	ML2-AH-16	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.		
	ML2-AH-17	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.		