MND Family Third Party Risk Management Programme (TPRM)

Restricted \ Non-Sensitive

Most cyber incidents that affected MND Family in recent years were due to Vendor/Partner Incidents

Problem Statement for TPRM Programme

As Govt systems are reasonably protected, we can expect attackers to target our Third Party vendors/systems, which are less well defended. Further, breaches may not be known and reported.

TPRM is designed to enable agencies to establish adequate oversight over Third Parties:

- Risk assessment at the start of all Projects.
- Certification in Cyber Hygiene and Data Protection.
- Continuous Monitoring of Vendor Performance

TPRM Expectations for Vendors/Research Partners

- Infosecurity Hygiene Certifications
  - Cyber Essentials (CTE)
  - Cyber Trust Mark (CTM)
- Data Hygiene Certifications
  - Data Protection Essentials (DPE)
  - Data Protection Trust Mark (DPTM)
- Demonstrate above hygiene in daily work as advised by certifying companies.

		Cyber Trust Mark				
	Cyber Essentials	Tier 1: Supporter	Tier 2: Practitioner	Tier 3: Promoter	Tier 4: Performer	Tier 5: Advocate
Cyber Governance and Oversight						
1. Governance				●	●	●
2. Policies and procedures				●	●	●
3. Risk management		●	●	●	●	●
4. Cyber strategy						●
5. Compliance		●	●	●	●	●
6. Audit					●	●
Cyber Education						
7. Training and awareness*	●	●	●	●	●	●
Information Asset Protection						
8. Asset management*	●	●	●	●	●	●
9. Data protection and privacy*	●	●	●	●	●	●
10. Backups*	●	●	●	●	●	●
11. Bring Your Own Device (BYOD)					●	●
12. System security*	●	●	●	●	●	●
13. Anti-virus/Anti-malware*	●	●	●	●	●	●
14. Secure Software Development Life Cycle (SDLC)						●
Secure Access and Environment						
15. Access control*	●	●	●	●	●	●
16. Cyber threat management					●	●
17. Third-party risk and oversight						●
18. Vulnerability assessment				●	●	●
19. Physical/environmental security			●	●	●	●
20. Network security			●	●	●	●
Cybersecurity Resilience						
21. Incident response*	●	●	●	●	●	●
22. Business continuity/disaster recovery			●	●	●	●
	8 DOMAINS	10 DOMAINS	13 DOMAINS	16 DOMAINS	19 DOMAINS	22 DOMAINS

DPE

1: Register your DPO with ACRA/PDPC
2: Take inventory of your organisation's personal/biz critical data, hardware and software, accounts
3: Establish your organisation's data protection and security governance policies
4: Develop an incident response and data breach management plan
5: Complete Data Protection and Cybersecurity training set out for employees
6: Implement Data Protection and Cybersecurity measures

DPTM

Principle 1: Governance and Transparency
A: Establish data protection policies and practices
B: Establish queries, complaints and dispute resolution handling processes
C: Establish processes to identify, assess and address data protection
D: Establish a data breach management plan
E: Accountability
F: Internal Communication and Training
Principle 2: Management of Personal Data
A: Appropriate Purpose
B: Appropriate Consent
C: Appropriate Use and Disclosure
D: Compliant Overseas Transfer
Principle 3: Care of Personal Data
A: Appropriate Protection
B: Appropriate Retention and Disposal
C: Accurate and Complete Records
Principle 4: Individual's Rights
A: Effect Withdrawal of Consent
B: Provide Access and Correction Rights

How to Get Certified

- Cyber Hygiene Certification (from CSA)
  - https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-scheme-for-organisation
- Data Hygiene Certification (from IMDA)
  - https://www.imda.gov.sg/how-we-can-help/data-protection-essentials
  - https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification/
- Your company may be eligible for grants/subsidies for the 2 certification. Please contact CSA and IMDA for more details.

The End