

**PRINT THIS PAGE, COMPLETE FULLY AND ATTACH TO YOUR
WARRANTY REIMBURSEMENT REQUEST(S)!!!!**

Minimum Cyber Controls

The following is checklist of the minimum cyber security controls required to be in-place (implemented) on the affected system or SaaS Portals or by the affected person prior to a Cyber Warranty Event:

Review all requirements regularly to ensure warranty event requirements are met.

- Did you have anti-virus and/or anti-malware software implemented on all desktops, laptops, and Sensitive Systems (all systems (including all hardware, software and physical components thereof and the data stored thereon) visible to external networks and/or used to store/process non-public, confidential, proprietary, or POPIA related information) running a Microsoft operating system and up to date as per the software providers' recommendations?
 - Yes
 - No
- Did you have Critical, Common Vulnerability Scoring System (CVSS) severity 9.0-10.0, security related patches and updates applied on Sensitive Systems within 1 (one) months of release by the provider?
 - Yes
 - No
- Did you have the following password controls implemented on Sensitive Systems:
 1. *Password length of at least 8 (eight) characters?*
 - Yes
 - No
 2. *User account password configured to be changed at least every 120 (one hundred and twenty) days unless passwords are at least 14 (fourteen) characters in length or multi factor authentication is implemented?*
 - Yes
 - No
 3. *Passwords configured which cannot within reason be deemed widely used or easily guessable e.g., including the Client's name or P@ssword1?*
 - Yes
 - No
 4. *User accounts configured to lockout because of at most 10 (ten) failed authentication attempts?*
 - Yes
 - No

- Did you have the following recovery controls in place at the time of the cyber event:
 1. *Backups generated at least weekly or have replication implemented?*
 - Yes
 - No
 2. *At any point in time have a backup or replicated copy which is disconnected, offline or cannot be overwritten from the production environment?*
 - Yes
 - No
 3. *Testing of the ability to restore data from backups or read from replicated copies at least every six (6) months?*
 - Yes
 - No
- If your computer system includes a company network, did you have the following in place at the time of the cyber event:
 1. *Firewalls configured to restrict access to digitally stored sensitive Information?*
 - Yes
 - No
 2. *Administrative/remote access interfaces such as Remote Desktop Protocol (RDP) are not accessible via the open internet. Where such interfaces are required, these are accessible exclusively over secured channels such as Zero Trust Network Access (ZTNA), Multi-factor authentication (MFA) or Virtual Private Network (VPN) connections?*
 - Yes
 - No
 3. *The system and/or activity logs for all Sensitive Systems including firewalls and Active Directory as implemented in the Client's environment stored for a minimum period of 1 (one) month?*
 - Yes
 - No
- Did you have email security protocols implemented for your email domain at the time of the cyber event:
 1. *Domain-based Message Authentication, Reporting, and Conformance (DMARC)?*
 - Yes
 - No

2. Mail Transfer Agent Strict Transport Security (**MTA-STS**) to enforce Transport Layer Security (**TLS**) encryption for email transmission between servers, preventing interception and ensuring secure communication?

Yes

No

○ Did you have data encryption and access control (quarantine or lockout) measures in-place for any lost, stolen or compromised devices holding sensitive data on computers, USB storage drives or mobile devices in place at the time of the cyber event?

Yes

No

○ Did you provide sufficient cyber awareness training to computer users and have a cybersecurity awareness training program in place at the time of the cyber event?

Yes

No

○ Did you provide an option for users to confirm recipients when sending emails which contain sensitive data to avoid such emails being sent to the wrong people at the time of the cyber event?

Yes

No

○ Did you provide an option for users to encrypt and password protect correspondence which contain sensitive data to prevent unauthorised access during transit or when such correspondence is stored on recipient devices at the time of the cyber event?

Yes

No

Checklist Completed By:

FULL NAME :

JOB TITLE :

CONTACT EMAIL ADDRESS :

CONTACT MOBILE NUMBER :