MoverOne
INTERNATIONAL

Cyber Security and Risk Management

1. Risk Management:

The following policies address how risk is assessed in order to implement security measures, prioritizing the biggest threats, and ensuring appropriate responsiveness:

8 - Incident Response 2022.docx
14 - Security Assessment & Authorization.docx
16 - IT Security Risk Assessment Policy 2022.docx
Incident Response Plan.docx

2. Secure configuration:

To ensure proper configuration, avoid data breaches, removal or disabling or unnecessary system functions, and to address known vulnerabilities promptly, we use MS ATP, Manage Engine Patch Management, and RBAC on all our systems.

3. Home and mobile working:

Bitlocker is installed on all our endpoints and MFA is mandatory for all remote access

4. Incident management:

To quickly respond to a security incident, mitigate damage and to get back-up running as quickly as possible, the Incident Response Plan is put into action as well as VEEAM backup saves to secondary Linux NAS and replicates to inactive Offsite DR Facilities.

5. Malware prevention:

We employ Knowbe4 training and reporting, and use MS ATP for incident prevention and Malware detection.

6. Managing user access:

To ensure that our staff can only access information that is relevant to their job, we utilize AD security groups and application groups (RBAC). End users cannot install applications and require approval to install sensitive applications.

7. Monitoring:

To monitor our systems to identify incidents promptly and to initiate response efforts, MS Advanced Threat Protection (ATP) Is used on all our endpoints and servers.

8. Network security:

To reduce the likelihood of our networks connection to the internet being exploited, we use Meraki Threat protection on our firewall NATs and MS ATP on the servers.

9. Removable media controls:

To emphasize the need to digitally, as well as physically, protect removable devices in order to avoid and reduce security issues, we have servers located in a restricted datacenter that requires biometric authentication and are further physically locked in a cabinet requiring a combination. AD group polices grant access to certain info with MFA on all remote access. MS ATP scans all removable media upon insertion. Endpoints are locked by group policy after 5 minutes of inactivity to protect data.

10. Accountability, user education and awareness:

To create awareness, as well as to educate our staff, on how to achieve an effective Cyber Security environment we employ Knowbe4 training videos, monthly phishing tests, and quizzes/training are given to end users.

Our IT System Admin is responsible for all items related to Cyber Security Management

Our company monitors and reviews our procedures at least once a year to ensure that effective cybersecurity management is achieved by mitigating the risk of cyber-crime. Coalition Inc. runs yearly Reviews on our cybersecurity. In 2022 we contracted a Third party GAP analysis through Vulnerability Scout to review our policies and recommend updates, which were carried out.

To demonstrate that our Cyber Security Management procedure has been communicated to internal personnel, there are reports available that show monthly phishing tests are conducted and a training register showing that staff have been informed and adequately trained on Cyber Security through use of training videos.