Newable

Newable Cyber Security Strategy

Version 4

January 2021

06 APRIL 2021

Newable

Version Control

Version	Owner	Reviewer	Changes	Date	Next Review
1.0	Michael Walsh	Mashudul Karim	Initial version	06/2017	04/2018
2.0	Michael Walsh	Mashudul Karim	Changed membership	04/2018	04/2019
3.0	Michael Walsh	Mashudul Karim	Added version control, revised frequency of meetings, removed review of training statistics	10/2019	05/2020
4.0	Michael Walsh	Mashudul Karim	Added reference to Risk Appetite Statement, clarified scope, updated members, added new policies	01/2021	01/2022

Newable

Background

Newable as a business has determined that it has a low appetite for operational risk and its Risk and Governance Committee has communicated this clearly in a Risk Appetite Statement, which outlines the following types of operational risk:

I. Information Security
II. Cyber Security
III. Change Management
IV. Third Party Suppliers

The Cyber Security Committee (CSC) is a formal subcommittee of the Risk and Governance Committee and it is charged with developing, overseeing and governing the implementation of an effective cyber security strategy, for Newable Limited and its wholly-owned or majority-owned entities (subsidiaries), in accordance with the Risk Appetite Statement.

The purpose of this document is to establish and articulate the cyber security strategy developed by the CSC to achieve its objective of maintaining a robust cyber security environment commensurate with known and potential cyber threats.

The CSC is responsible for communicating this strategy as and when appropriate and ensuring the timely and successful delivery of all programmes of work outlined herein.

Newable

Approach

The CSC recognises that information technology is both a critical internal resource and, increasingly, a valuable competitive differentiator. It also recognises that Newable and many of its subsidiaries operate in industries where they act as a trusted adviser, have a relatively high profile, undertake regulated activities or deliver significant contracts on behalf of the UK Government or other public bodies.

There is a risk that a cyber-security event could cause disruption and reputational damage that may impede the business affected from operating effectively in the short term, limit some of its activities in the medium term or preclude it from offering certain services entirely in the future.

In developing this strategy, the CSC has balanced the need to mitigate the risk of a cyber-security event with the need to allow Newable and its subsidiaries to innovate and develop new products and services to serve their clients better. In practical terms, this means that the CSC has assessed each policy, control or programme of work outlined in this strategy on a case-by-case basis to ensure that it is proportionate to the cyber risk it seeks to address.

Newable

Assessing and measuring risks

The CSC assesses and measures risks through the following mechanisms:

1. Review of incidents and exceptions (to policies, procedures or controls) four times a year
2. Review of updates and reports from subsidiaries four times a year
3. Review of Third Party Assurance registers four times a year
4. Review of the Newable Digital Risk Register four times a year
5. Vulnerability scans and penetration tests by an accredited third party once a year
6. A disaster recovery test for Newable undertaken by Newable Digital once a year and independently reviewed by the Crisis Management Team
7. A disaster recovery test for each subsidiary undertaken by suitably trained staff once a year and independently reviewed by Newable Digital
8. An internal audit of Newable Digital by an independent body once every two years
9. An internal audit of each subsidiary by Newable Digital or an independent body once every two years
10. Periodic reviews (including physical site visits) of key third parties to ensure that they manage security and associated risks adequately (with mandatory reviews and approval before contractual engagement)

Maintaining a low risk profile

The CSC maintains a low risk profile for Newable and its subsidiaries through a combination of oversight (including reporting), policies, controls and training.

Oversight

The CSC is the primary body providing oversight of the cyber security agenda and its remit includes Newable Limited and all wholly-owned and majority-owned entities. It meets four times a year and comprises the following members:

- Michael Walsh, Chief Financial Officer (Chair)
- Joanne Wilkinson, Head of Compliance, MLRO and DPO (Deputy Chair)
- Monica Whitefield, Chief People Officer
- Mashudul Karim, Chief Information Officer
- Brendon Simpson, Head of Risk
- Ruth Collier, Group Head of Marketing
- Gavin Holland, Head of Business Systems and Process
- Lisa Richardson, People, Policy & Productivity Director, NewFlex
- A representative from BDO who are the current auditors of Newable Limited and who attend meetings at least once a year
- Other members are appointed from time to time as required

In addition, the CSC is a formal subcommittee of the Risk and Governance Committee, which meets three times a year, and provides a reports on its activities to that body once a year.

Policies

In order to ensure that there is an effective framework for Newable to maintain a low risk profile, the CSC maintains, communicates and enforces the following policies:

- Newable Information Security Policy
- NewFlex Information Security Policy
- Newable Third Party Assurance Policy
- Newable Digital - Service Level Agreement
- Newable Digital - Access Policy
- Newable Digital - Backup Policy
- Newable Digital - Build Policy
- Newable Digital - Logging Policy
- Newable Digital - Update Policy

Newable

The CSC reviews each of the policies once a year with additional reviews whenever there is a substantial or material change within the business or the wider threat level.

The CSC provides copies of the policies to each subsidiary as templates and there is a reasonable degree of flexibility for each business to adapt them to suit their business environment or operating model.

However, in order to ensure consistency and a de minimus level of mitigation against cyber risks, the CSC reserves the right to review and approve all proposed changes to policy and, in exceptional circumstances, may reject any changes that it believes would compromise standards.

Controls

As part of its remit, the CSC regularly reviews and assesses the effectiveness of physical and logical controls to prevent, detect and mitigate security threats.

This work extends to strengthening existing controls and introducing new controls where necessary to maintain a robust cyber security environment commensurate with known and potential cyber threats.

Physical controls include (but are not limited to):

- Restrictions on access to locations, areas and rooms containing sensitive information, assets and equipment
- Restrictions on the transfer of sensitive information, assets and equipment between locations
- Closed-circuit television recording and/or private security personnel at locations containing high-value information, assets and equipment

Logical controls include (but are not limited to):

- Uniquely identifiable accounts for information technology users and separate, uniquely identifiable accounts for information technology administrators
- Passwords with mandatory complexity requirements and limits on age and reuse
- Multi-factor authentication (including one-time codes sent to mobile phones or other devices)
- Access control lists with strict separation (i.e., no inheritance or nesting of permissions)
- Firewalls and other threat management systems (for intrusion detection and prevention)
- Antivirus software with daily and on-demand definition updates
- Automatic software updates and patching
- Encryption of local storage to industry and/or government standards
- Encryption of remote access gateways, endpoints and externally accessible websites
- Comprehensive inventory of information, assets and equipment

Newable

Training

The CSC recognises the importance of staff training in raising awareness of cyber security threats, encouraging best practice and affording a basic level of protection to Newable and its subsidiaries at the point of maximum exposure (where staff are most likely to engage with the public and third parties).

To that end, the CSC assesses the availability and effectiveness of cyber security training across the business and this includes a detailed review of providers, materials and methods at least once a year.

Newable

Summary

The purpose of this document was to establish unambiguously that Newable:

- has a low appetite for cyber risk in line with its appetite for operational risk and as communicated in its Risk Appetite Statement;
- assesses and measures its risk profile through a comprehensive programme of regular reviews, audits and tests; and
- maintains its risk profile at an acceptable level through a combination of oversight, policies, controls and training.

The CSC plays an active role in shaping the corporate response to cyber security threats and keeping the Board and the Risk and Governance Committee informed of its performance against key performance indicators and the status of all security controls.