Business Continuity Plan – Annual Review

Purpose: **Approval**

Author: **Head of Executive Office**

Approver: **Chief Executive**

Summary

This report reviews the CLC's Business Continuity Plan which was last updated in October 2023, having been reviewed extensively to place greater emphasis on the ways of working that have been in place since the pandemic and in particular to reflect IT risks.

Since revision of the Business Continuity Plan, Multi-Factor Authentication (MFA) for access to CLC equipment and software has been introduced. MFA enables equipment and access to systems to be de-activated remotely.

There is ongoing walkthrough scenario testing being undertaken and any significant results will be reported back to ARC with any suggested amendments to the BCP which can be done outside of the regular review cycle.

The Committee is invited to approve the Business Continuity Plan attached at **Appendix A**, which was considered by the Audit and Risk Committee at its meeting on 16 July 2024, which is recommending it for adoption. The Committee recommended the inclusion of the following amendments which have been incorporated at sections 4 (Business Continuity Risk Assessment) and Appendix I (Social Media Breaches):

- Business Continuity Risk Assessment – clarification that Data Breach risks are not limited to cyber attack or sabotage and may result from human error as an example
- Appendix I – Social Media - inclusion of the CLC's Communications provider as a contact for rectification of social media issues.

Recommendations

Council is asked to review and approve the attached Business Continuity Plan.

Risk management

The purpose of the Business Continuity Plan is to mitigate risks to the effective operation of CLC business in the event of a serious incident, such as a major security alert, weather disruption affecting access to the office premises or lose of IT systems.

Regulatory Objectives

The preparation and adoption of a comprehensive BCP enhances the CLC's ability to be able to achieve all the regulatory objectives even in adverse circumstances.

Financial impact

There are no financial considerations specific to this report, however any implementation of additional IT controls or other mitigations are likely to have a financial impact.

Diversity and inclusion impact

There are no diversity and inclusion considerations specific to this report.

Communications requirements

Contact information for CLC staff is updated regularly.

All staff have access to the WeWork Emergency Response Guide and the Data Breach Policy and Reporting procedure, receive regular training on IT security, data breach awareness and reporting and participate in premises evacuation drills.

Any amendments which are made to the Business Continuity Plan will be communicated to staff in writing and at staff meetings.

Publication

Not for publication. The Business Continuity Plan contains personal information.

Annex A

The CLC Business Continuity Plan