Committee(s)	Dated:
Summit Digital Services Sub Committee (DSSC)	26th November 2019 24th January 2020
Subject: City of London Corporation Information Handling (Protective Marking)	**Public**
Report of: Michael Cogher - Comptroller Peter Kane - Chamberlain	**Summit for Decision** **DSSC for Information**
Report authors: Sean Green – IT Director	

Summary

The Information Management (IM) Strategy was agreed by Summit in March 2019 and the Digital Services Sub-Committee in July 2019.

A Corporate risk was developed in March 2019 (see Appendix A below) that recognises the cultural and maturity issues the organisation faces currently with how we manage and support good information management curation and practices.

This paper presents the proposal to implement a protective marking schema in the organisation which, based on our current Microsoft licencing, will initially be manually applied however with future licence investment in 20/21 much of this can also be automated.

Recommendation(s)

Members are asked to:

- Note this report.

Main Report

Background

1. In March 2018 Summit agreed the IM Strategy

2. The strategy seeks to transform IM capabilities (tools and skills) and culture (values and behaviours) across CoL and its partners so that accurate and timely information is routinely and effectively used as the basis for decisions and actions, thereby leading to better service outcomes.

3. When the IM Strategy was presented to Summit in March 2019 it was recognised that a corporate risk should be created (See Appendix A attached)

4. Protective Marking came into effect in April 2014 and describes how HM Government classifies information assets to ensure they are appropriately

protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations.

5. The Government's protective marking system is designed to help individuals determine, and indicate to others, the levels of protection required to help prevent the compromise of valuable or sensitive assets. The markings signal quickly and unambiguously, the value of an asset and the level of protection it needs.

6. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.

7. The City of London Police applies security classification to all documents and emails internally and externally and has been in force for many years.

8. The use of the protective marking schemas in of itself can change the culture of how staff perceive and value the information that they manage on behalf of the organisation. This would be the main benefit that would accrue to CoL.

9. As we move to a more flexible model of remote working from smaller locations and home the potential for in appropriate handling and release of sensitive information could increase therefore the cultural impact that protective marking should bring about should be of benefit to CoL.

10. In summary implementing a simplified protective marking scheme improves our information security and supports the mitigating actions for CR29 (see Appendix A attached).

Proposal for Implementation of Protective Marking

11. It has been agreed by Summit that CoL will apply protective labelling in a more pragmatic and practical way than the standard definitions provided by National Government with 2 labels and sub-categories that staff can choose that will be both be applied in the header, footer and watermark of the document

12. 3 labels can be chosen from a drop-down list:

    a. Official – All routine public-sector business, operations and services should be treated as OFFICIAL;
    b. Official Sensitive – A limited subset of OFFICIAL – information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media.

       Note: Anything not marked will be considered as Non-business data for personal use only;

13. When Official Sensitive is chosen any email used to send the document will be encrypted. In addition, for this category there are 3 sub-categories that the member of staff will be offered from a drop-down list which are:
    a. Internal only – Will be encrypted so that it can only be opened with internal organisational email address or through whitelisted email addresses or domains;
    b. Commercial – Email or document can be externally sent and opened but will be encrypted.
    c. Personal Data – Contains personal data as defined by the data protection act. Can be sent externally but will be encrypted.

14. The process for applying labels to documents will be manual with a recommended default to 'official' as a public-sector organisation we subscribe to a policy of openness and transparency.

15. To ensure officers, recognise the role of the Communications Director and his team for the release of any CoL information with any public forum a new footer will be added to all CoL documents that states:

    ''This information remains the property of the City of London Corporation. Any requests to share this information in a public forum should be made through the City of London's Communication team'

16. Alongside the small system changes there will be online training and an information management cultural change and communication campaign.

17. In the future when we upgrade our current Microsoft licences, we can automate the application of protective marking labels based on sensitive and personal data detected in documents using Artificial Intelligence rules.

Next Steps

18. Following launch of Protective Marking staff will be encouraged to undertake short training course and explanation of the benefits of the using the schema will be communicated through communication campaigns.

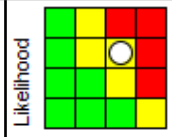
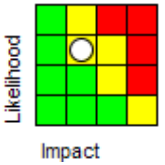
19. Feedback and use of Protective Marking and Information Handling will be sought 3 months after launch to evidence mitigation of the Corporate IM risk.

20. Further automation (using AI rules) and protection of sensitive data should be implemented in 2020 following proposed upgrades to the organisation's Microsoft Office licences.

IT Director
Chamberlain's Department
E: Sean.Green@cityoflondon.gov.uk

Appendences
Appendix A – IM Corporate Risk

Appendix A – IM Corporate Risk

Risk no, title, creation date, owner	Risk Description (Cause, Event, Impact)	Current Risk Rating & Score		Risk Update and date of update	Target Risk Rating & Score		Target Date	Current Risk score change indicator
CR29 Information Management 08-Apr-2019 John Barradell	**Cause:** Lack of officer commitment and investment of the right resources into organisational information management systems and culture. **Event:** The City Corporation's IM Strategy (2018-2023) is not fully and effectively implemented **Effect:** • Not being able to use relevant information to draw insights and intelligence and support good decision-making • Vulnerability to personal data and other information rights breaches and non-compliance with possible ICO fines or other legal action • Waste of resources storing information beyond usefulness		**12**	• New business intelligence dashboards continue to be developed for improved decision making by the Corporate Strategy and Performance team • An Information Management Awareness campaign starts from 19 February to 12 March. • Work will begin to review relevant staff roles that should have an information management competency added • A paper covering the benefits and proposed implementation of Protective was agreed by Summit in their December meeting • Capital bids submitted for information management investment to support the mitigation of this risk **11 Dec 2019**		**6**	30-Jun-2020	Constant