UNIVERSITY OF CAMBRIDGE
Information Services

Security Guidance for Dropbox

1. Context

This guidance is for the Dropbox (Professional & Business editions) service, & helps you Understand what data can be stored within this Public Cloud Service, and what classifications of data Dropbox can hold on the basis of the current University Guidance on Data Security Classification. Personal Dropbox accounts are not covered by this documentation, & as such are not authorised for holding University of Cambridge data.

Similar guidance may apply to other devices you use to store this data and appropriate protections may be necessary on those devices. You should seek out and become familiar with such guidance. It is assumed here that you are already familiar with that guidance.

We have also taken into account the current UK Government Classification system in order to provide additional information and assurance for you to ascertain what data will be appropriate for storage within this Public Cloud Service.

Both sets of Classification and Guidance are being provided because of the broad usefulness of the current UK Government Guidelines, which are in use throughout the UK public sector and which have established and considered application in the use of Public Cloud Services. The UK Government Guidelines are provided in Appendix 1 for reference.

It is important to note, in all levels of security classification, the principal factor in good data management is the 'Need to Know' principle (Information is only shared to people who need to know the information).

2. University Data Security Classifications & Guidelines

The University Guidance defines the following classifications.

Level 0: Unclassified or public information

Unclassified or public information is the largest class containing the majority of information.

Level 1: Cambridge Only

This covers information that is only available to students and staff within the Cambridge domain. It includes memoranda, minutes of meetings (not otherwise marked), and site-licensed software.

Level 2: Confidential information

This covers certain minutes of meetings, general personal information, financial information, or other information designated as confidential but that may be dealt with by any staff with delegated responsibility from the recipient (i.e. it is not, in a strict sense, information 'for your eyes only').

Level 3: Personal and strictly confidential information

This covers documents that contain highly sensitive information or personal details that are for the eyes of the recipient only where delegated authority is not appropriate.

Application to Dropbox

The Dropbox Agreement includes Terms and Conditions that are compliant with UK/EU Data Protection Law and the University Statutes and Ordinances. Dropbox provides EU Model clauses in agreements and hold ISO 27001 certification. The data centres are located in the EU. The Services offered are integrated with authentication processes entirely within the control of the University of Cambridge.

Staff should note that specific contractual obligations applying to aspects of their work may supersede this guidance and those obligations should be treated as exceptions. Staff should ensure they are aware of any contractual obligations and treat those as having precedence; if in doubt, staff should seek guidance from local Data Protection Officers.

Hence the current policy on the use of Dropbox is:

Subject only to the exclusions below, data under Data Classification Levels 0, 1 and 2 above CAN be stored in Dropbox.

Data excluded from the above includes:

- Data classified as Level 3 above,
- Patient Identifiable Data (including other identifiable data which is subject to the Clinical School's mandatory data security policy which can be found at http://www.medschl.cam.ac.uk/research/information-governance/),
- Data that is subject to a specific contractual agreement that specifies a particular storage method (that is not Dropbox),
- Data that is subject to a specific contractual agreement that prohibits storage in a Public Cloud Service.

Such data MUST NOT be stored in Dropbox.

UNIVERSITY OF CAMBRIDGE
Information Services

3. Incident Reporting

Any breach (loss of data, unauthorised access, 'over-sharing' or any other security incident) must be reported to:

- Local or Institutional Data Protection Officers,
- The University's Information Compliance Office (contact details can be found at http://www.information-compliance.admin.cam.ac.uk/contact-us)
- The UIS (incident reporting guidelines can be found at http://www.informationmanagement.admin.cam.ac.uk/incident-reporting)

4. Further Information

For further information on classification of data or if you are unsure if your data may fall into an excluded category please contact informationmanagement@uis.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Information Services

Appendix 1

UK Government Security Classifications & Guidelines

This section provides an overview of the current UK Government Security Classification Policy. For further detailed information, refer to the Cabinet Office documentation which can be found at:

https://www.gov.uk/government/publications/government-security-classifications

These classifications provide guidance and data owners should take into account whether any other requirements and restrictions are in place that may provide additional constraints, for example NHS Data Sharing agreements and NHS Patient Data classification.

The Security Classifications are (in ascending order):

OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business, operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but which are not subject to a heightened threat profile of the organisation or people within, for example:

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

There is no requirement to explicitly mark routine OFFICIAL information, as the baseline security standard of the organisation should be enforced through local processes.

Information of this Security Classification CAN be stored in Dropbox.

OFFICIAL-SENSITIVE

There is an additional security caveat of SENSITIVE that can be added to the security classification of OFFICIAL. This caveat states to the all data controllers and

handlers that the information contained within, if lost, stolen or published in the media, would have damaging consequences. It is important to note, that this information is still handled as the same requirements as OFFICIAL, but is an additional statement to say there is a clear and justifiable requirement to reinforce the 'Need to know' principle.

Information of this Security Classification CAN be stored in Dropbox.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined and high capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime. For example, the loss of Secret information might:

- Directly threaten an individual's life, liberty or safety (from highly capable threat actors).
- Cause serious damage to the operational effectiveness or security of UK or allied forces such that in the delivery of the Military tasks:
- Current or future capability would be rendered unusable;
    - Lives would be lost; or,
    - Damage would be caused to installations rendering them unusable.
- Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.
- Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.
- Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.
- Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.
- Cause major impairment to the ability to investigate or prosecute serious organised crime.

All information within this domain must be clearly and conspicuously marked 'SECRET'. It is common that information of this protective marking may require special handling instructions. Information on these requirements are not in the scope

of this document, and are available on the Cabinet Office guidelines at https://www.gov.uk/government/publications/government-security-classifications.

Information of this security classification MUST NOT be stored on Dropbox (or any non-authorised system or network).

TOP SECRET

This is Her Majesty's Governments most sensitive information, requiring the highest levels of protection from the most serious threats. For example, where compromises could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. Loss of Top Secret information might:

- Lead directly to widespread loss of life.
- Threaten directly the internal stability of the UK or friendly nations.
- Raise international tension.
- Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Military Tasks.
- Cause exceptionally grave damage to relations with friendly nations.
- Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.
- Cause long term damage to the UK economy.
- Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.

The classifications for SECRET provide the baseline of personnel, physical and information security controls that offer an appropriate level of protection. The university may need to apply controls above (or below) the baseline on a risk managed basis appropriate to local circumstances in line with HMG risk tolerances. The Senior Information Risk Owner (SIRO) will moderate such instances as required.

All information should be clearly and conspicuously marked as TOP SECRET. This information may, like SECRET, have further restrictions.

Information of this security classification MUST NOT be stored on Dropbox (or any non-authorised system or network).

Descriptors

Along with the addition of OFFICIAL-SENSITIVE, descriptors are also used in order to limit distribution and indicate the need for common sense precautions to limit access. Common descriptors that maybe used within the University of Cambridge maybe the following

- **COMMERCIAL** – This is commercial or market sensitive information, including that subject to statutory or regulatory obligations, that maybe damaging to HMG or a commercial partner if improperly accessed.
- **PERSONAL** – Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. A few examples of where this descriptor will come into force would be when relating to ongoing investigations, vulnerable individuals, etc.
- **MEDICAL** – Information contained within is of a medical nature (e.g. could be Patient Identifiable Data).

In a cloud environment, this means that any data that has these descriptors, should only be viewed by people that "Need to Know" such information.

Application to Dropbox

Dropbox for Business ("Dropbox") is an assured G-Cloud Public Service.

Dropbox provide EU Model clauses in agreements, hold ISO 27001 certifications and operate their data centres within the **United States**. This means, in practice, that Dropbox is cleared to host data with the classification of OFFICIAL.

However, whilst Dropbox can host the data, information of this classification still requires sound knowledge of handling procedures and effective security processes.

Under this method of Classification, the policy on the use of Dropbox would be:

Subject only to the exclusions below, data classified as OFFICIAL CAN be stored in Dropbox.

Data excluded from the above includes:

- Patient Identifiable Data (including other identifiable data which is subject to the Clinical School's mandatory data security policy issued under the HSCIC-compliant Information Governance Toolkit documented at http://www.medschl.cam.ac.uk/research/information-governance/),
- Data that is subject to a specific contractual agreement that specifies a particular storage method (which is not Dropbox),
- Data that is subject to a specific contractual agreement that prohibits storage in a Public Cloud Service.

UNIVERSITY OF CAMBRIDGE
Information Services

Such data MUST NOT be stored in Dropbox.