# Information Security Directive

# Protecting Sensitive IT Vulnerability Data

# Brunel University London

***An ISO/IEC 27001:2013:*** *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

**Mick Jenkins**

Chief Information Security officer

# Document History

| Version | Author | Comments | Date |
|---|---|---|---|
| V 0.1 | Michael Jenkins | Initial Draft | 22/05/2019 |
| V 1.0 | Michael Jenkins | Formatting changes | 26/06/2019 |
| V 1.0 | Andrew Clarke | Annual review | 22/06/2020 |

## Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

| | |
|---|---|
| Owner: Michael Jenkins | Chief Information Security Officer |
| Signature: MGJ | Date: 26 Jun 2019 |
| Distribution: | ALL |
| | |
| | |
| | |
| | |
| | |

This document requires the approval from BUL as defined in the ISMS Compliance document.

## Protecting Sensitive IT Vulnerability and Cyber Security Information

University information, whether databases, spreadsheets or text documents, that contain sensitive information relating to ***identified IT vulnerabilities, risks and threats*** must be classified as University Confidential in accordance with the Information Classification Policy and handled in accordance with the Information Classification Process

The information asset owner for all these documents is the CIO.

The classification UNIVERSITY CONFIDENTIAL "descriptor" must be included in the document at the middle, top or bottom of every page, which must be manually set to appear on all pages of the document, or on the media on which it is recorded.

## Impact of Compromise

A breach of this information could result in unacceptable damage with very serious and lasting consequences threatening the University or one of its activities, its staff along with significant financial and reputational costs.

If third party access is required, either for handling the information on behalf of the University, or processing the information, the third party shall be required by contract to adhere to this policy prior to the sharing of information.

PROTECT ANY DOCUMENTATION THAT IDENTIFIES OUR IT VULNERABILITIES

## Information Handling and Storage

Email:

- Internal:
    - University email marked UNIVERSITY CONFIDENTIAL in the subject line;
    - Email should be tagged with a Confidential sensitivity.
    - Number of addressees should be limited and only sent to those parties that have a requirement for this information. Do not send such emails to group email addresses – send them to named individuals;
    - When forwarding or replying, consider whether all of the addressees need to see the entire email thread, or see the attachment. If the entire email thread is not required, delete the unneeded communications.
    - When sending an email try not to include the particular text relating to the vulnerability, risk or threat in question within the body of the email, send the data as an attachment.

- External Email:
    - labelled and managed as above, only sent to appropriate organisation, stakeholder or recipient
    - When sending an email containing an attachment, ensure that the attachment is encrypted with a complex password compliant with the University Password Policy using the recommended University compression and encrypting tool and can only be sent to the email box(es) of the

identified recipient(s) and may not be copied or forwarded to individuals or roles that are not authorised to receive it;

**Printing**: Only print on University provided managed-print devices that can authenticate the printing of the document. Ensure that all pages are recovered from the device;

**Storage of papers**: Keep protected in a locked cabinet or drawer. Do not leave unattended at any time;

**Disposal of papers**: Secure waste disposal (provided storage bins) or by shredding;

**Electronic storage**: University's network drives, SharePoint or University Office 365 OneDrive for business and Office 365 Groups: restricted access by defined user/user groups to specific areas.

**Personal removable and storage media**: Not to be saved on personal removable and storage media (CD-ROMS, USB storage), exceptions only those provided by the University – must be encrypted to at least 256-bit AES cipher encryption and FIPS-140-2 level authorised by the CISO/CIO;

**Cloud storage**: *never* store in Cloud storage such as Dropbox, Google Drive, Copy, Box, MS OneDrive (personal), Sync.com, E-Box, Tresorit, owncloud, Viivio (except as above using University OneDrive for Business);

**Cloud communications**: *never* use Skype for business, Yammer, Sway and Forms

**Mobile Remote working**:

- Mobile devices must have Full Disc Encryption (FDE) using complex password;
- Do not save or print to local devices including USB portable devices;
- Do bit attempt remote access using public Wi-Fi networks (e.g. Starbucks, airports);
- Access only through remote Connect network access (VPN);

**Do not leave unattended on screen** - lock screen;

**Electronic media disposal**: Securely wipe then recycle or destruction if removable media;

**Public Website**: Not to be published on the Web

**Post**:

- Internal: Sealed envelope marked "[UNIVERSITY CONFIDENTIAL.] Addressee Only". Treated as current "Confidential" mail only to be opened by addressee;
- External: Sealed internal envelope showing classification, and sealed external envelope using Royal Mail 'Recorded Signed For' service or

preferably secure courier to named person, without security marking on the outside of the package, or delivery by hand;

- End -