| Title | Information Classification Scheme |
|---|---|

| Owner | Chief Information Security Officer (CISO) |
|---|---|

| Version | Version history | Version date |
|---|---|---|
| 1.0 | Reviewed and approved by CISO | 29 July 2016 |
| | | |
| | | |

## Preface and document control

This document is intended to support the University Information Security Policy and provides an information classification scheme and handling guidelines approved by the CISO. This document forms part of the University baseline requirements for information security and will be reviewed at least annually to ensure validity.

## 1 Information classification scheme

Information shall be classified according to the following scheme:

| Classification level | Examples | Rationale |
|---|---|---|
| **Confidential** | • Sensitive Personal Data<br>• Mass personal data relating to employees, students, alumni etc.<br>• Patient identifiable data<br>• Financial records and transactions<br>• Payment card data<br>• Sensitive research activities and Intellectual Property<br>• Examination papers & records<br>• Passwords | Need for confidentiality will far outweigh requirements for availability. Unauthorised disclosure may result in:<br>• Severe financial harm<br>• Long-term reputational damage<br>• Severe regulatory action<br>• Interruption of critical business system/processes<br>• Research contracts revoked<br>• Disbarment from future research bids<br>• Risks to the safety or wellbeing of personnel |
| **Internal (default)** | • Limited personal data (e.g. email addresses)<br>• Business information<br>• Information on Intranets<br>• Internal governance documents<br>• Meeting agendas & minutes<br>• IT network configuration & architecture<br>• Unpublished research papers<br>• Usernames and IDs | Unauthorised disclosure may result in:<br>• Financial harm<br>• Reputational damage<br>• Regulatory action<br>• Distress to personnel<br>• Impact on business systems/processes |
| **Public** | • Public internet information<br>• Brochures<br>• Prospectuses<br>• Published business reports<br>• Published academic & research reports<br>• Press releases (not under embargo) | • Unauthorised disclosure causes no harm<br>• Information likely already in the public domain<br>• Information is routinely published. |

## 2 Information Handling Guidelines

Information Asset Owners are responsible for Information Handling Rules. A set of typical rules per classification are presented below.

| Store, process, transmit… | Confidential | Internal | Public |
|---|---|---|---|
| **Where** | • Premises of organisation or highly trusted third parties (e.g. audited by accredited bodies and certified)<br>• University issued/controlled devices only | • Premises of organisation or trusted third parties (e.g. internally audited)<br>• Can be taken home with approval<br>• Personal devices in accordance with appropriate Acceptable Usage Policy | • Anywhere |
| **How** | • Approved methods only<br>• High levels of physically security with monitored access.<br>• Minimal number of copies permitted<br>• Audit trail of copies<br>• Additional security required over IT baselines.<br>• 2-factor authentication for remote access.<br>• Explicitly approved third parties with appropriate contractual agreements.<br>• Strict policies and procedures for secure disposal/deletion<br>• Encrypted in transit<br>• In accordance with appropriate retention schedule | • In accordance with baseline security standards<br>• Remote access permitted<br>• Contractual agreements for third party access<br>• In accordance with appropriate retention schedule | • Any method allowed<br>• In accordance with appropriate retention schedule |
| **Who** | • Tightly restricted groups of authorised persons only<br>• Approved and vetted third parties only<br>• Internal personnel may be vetted | • Authorised personnel (including third parties) only | • Anyone |