INFORMATION SECURITY POLICY

Title	Blavatnik School of Government Information Security Policy

Owner	Matthew Treavis
Approver(s)	Strategy & Resources Group (SRG)

Version	Version history	Version date
1	Initial draft	04/01/2017
1.1	For approval	11/07/2017
1.2	Approved at SRG	20/07/2017

Preface and document control

This document is intended to provide information security policy, procedure, standards or guidance in respect of Blavatnik School of Government and shall be reviewed at least annually to ensure validity.

Table of Contents

Purpose

This policy outlines the Blavatnik School of Government's approach to information security management and provides the guiding principles and responsibilities to ensure that the Blavatnik School of Government's security objectives are met.

Scope

This policy is applicable across the Blavatnik School of Government and individually applies to:

- all individuals who have access to Blavatnik School of Government information and technologies;
- all facilities, technologies and services that are used to process Blavatnik School of Government information;
- information processed, in any format, by the Blavatnik School of Government pursuant to its operational activities;
- internal and external processes used to process Blavatnik School of Government information; and
- external parties that provide information processing services to the Blavatnik School of Government.

Objectives

The Blavatnik School of Government's objectives for information security are that:

- a culture is embedded to ensure all teaching, research and administration activities consider information security;
- individuals are aware and kept informed of their information security responsibilities;
- information risks are identified, managed and mitigated to an acceptable level;
- authorised users can securely access information to perform their roles;
- facilities, technologies and services adequately balance usability and security;
- implemented security controls are pragmatic, effective and measurable;
- contractual, regulatory and legal obligations relating to information security are met; and
- incidents are effectively managed and resolved, and learnt from to improve our control environment.

Information Security Policy Framework (ISPF)

Information is critical to the Blavatnik School of Government operations and failure to protect information increases the risk of financial and reputational losses. The Blavatnik School of Government is committed to protecting information, in all its forms, from loss of **confidentiality**, **integrity** and **availability** ensuring that:

- all staff complete information security awareness training;
- information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;
- all relevant information security requirements of Blavatnik School of Government are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;
- appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store Blavatnik School of Government information;
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incidents properly investigated and managed;
- Information Asset Owners are identified for all Blavatnik School of Government information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place; and
- information security controls are monitored to ensure they are adequate and effective.

To provide the foundation of a pragmatic information security framework, the Blavatnik School of Government will implement a set of minimum information security controls, known as the baseline, either as published by the University's Information Security team or of equivalent strength. Where research, regulatory or national requirements exceed this baseline, controls will be increased at necessary service or project level. Where it is not possible or practicable to meet the baseline, exceptions will be documented to justify the deviation and appropriate compensating controls will be put in place. The baseline will support the Blavatnik School of Government in achieving its information security objectives.

The policy and the baseline shall be communicated to users and relevant external parties, and linked to from the website.

Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Strategy and Resources Group (SRG)** is accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within the Blavatnik School of Government.
- **The Chief Operating Officer (COO)** has executive responsibility for information security within Blavatnik School of Government. Specifically, the COO has responsibility for overseeing the management of the security risks to the Blavatnik School of Government's staff and students, its infrastructure and its information.
- **The Head of ICT** is responsible for establishing and maintaining the Blavatnik School of Government's information security management framework to ensure the availability, integrity and confidentiality of the Blavatnik School of Government's information. The Head of ICT will lead on the definition and implementation of the Blavatnik School of Government's information security arrangements.
- **Users** are responsible for making informed decisions to protect the information that they process.

Compliance

The Blavatnik School of Government shall conduct information security compliance and assurance activities, facilitated by the University's Information Security Team, to ensure information security objectives and the requirements of the ISPF are met. Wilful failure to comply with the policy and baseline will be treated extremely seriously by the Blavatnik School of Government and may result in enforcement action on a group and/or an individual.

Review and Development

This policy, and supporting ISPF documentation, shall be reviewed and updated by The Head of ICT and approved by SRG on an annual basis to ensure that they:

- remain operationally fit for purpose;
- reflect changes in technologies;
- are aligned to industry best practice; and
- support continued regulatory, contractual and legal compliance.