# INFORMATION SECURITY POLICY

**Introduction**

The Information Security Policy (ISP) details the principles and objectives that Brunel University London adopts in regard to Cyber and Information Security.

**Purpose**

The purpose of the Information Security Policy is to protect the Brunel University London and both our academics' and students' **Information Assets and Services** from all threats, whether internal or external, deliberate or accidental.

**Scope**

This policy applies to Brunel University London at Kingston Lane, Uxbridge and all associated sites;

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

**Objectives**

We, the management of Brunel University London, are committed to ensuring that:

- Brunel University will develop an Information Security framework aligned to university needs in order to establish strategic security objectives and will review these on a regular basis;

- Brunel University will maintain an Information Security framework to preserve its competitive edge, educational excellence, cash-flow, data protection, customer confidence and reputational image;

- Brunel University will ensure that the individuals, roles, bodies and governing frameworks are in place to maintain security ownership and responsibilities;

- Brunel University will continue to ensure that all authorised users can securely access information to perform their roles;

- Brunel University will use a risk based approach to ensure that information assets are identified and the confidentiality, integrity and availability are appropriately safeguarded by security controls;

- Brunel University will continue to comply with all relevant contractual, statutory and regulatory requirements that apply to information management;
- Brunel University as a university entity can survive with minimal disruption in the event of an Information Security breach occurring;
- Brunel University will treat all Personal Data as University Confidential;
- Brunel University will comply with the requirements of ISO 27001 and the guidance contained in ISO 27002 and maintain, as part of the overall Brunel University management system, an Information Security management system approach;
- Brunel University will ensure that all staff are aware of their responsibilities and obligations and are trained in how to respond in an Information Security scenario;
- Brunel University will pass security requirements on to our suppliers and customers to ensure consistency throughout the supply chain;
- Brunel University will maintain a Cyber Security incident management process in order to help protect the confidentiality and integrity of its information assets;

**Compliance**

Brunel University will regularly conduct information security compliance and assurance activities and Penetration testing to ensure information security objectives are met.

**Review**

The Information Security Policy and accompanying Information Security Management System Documentation shall be reviewed and updated on an annual basis to ensure that they:

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

*Professor Julia Buckingham, CBE, DSc, FRSB*
Vice-Chancellor and President, 07/08/2019

Reviewed: 01/08/2020