Volunteers, apprentices, and interns; and

failures of integrity[5] or interruption to the availability[6] of information, while allowing users to have access to University information and/or information technology services they require in order to carry out their studies and/or work.

4.2 As such, the University will:

4.2.1 Identify IT/cyber security threats which can affect the confidentiality, integrity or availability of IT assets through its cyber security tools (firewalls, event management systems, etc), various log entry files, Service Desk tickets and configuration databases.

4.2.2 Consider the potential threats applicable to IT assets, whether natural or human, accidental or malicious.

4.2.3 Assess the likelihood of IT security threats occurring and their potential impact.

4.2.4 Employ appropriate and proportionate measures to manage IT security threats in accordance with the Risk Management Framework, as well as any other relevant methodology (see section 3.5).

4.2.5 Monitor and review progress in managing threats.

4.3

4.3.1 The institutional Statement of Risk Appetite and Tolerance defines the amount and type of risk that the University of Sussex will take to achieve its objectives (risk appetite) and sets the parameters which determine the acceptance of risk (risk tolerance) without compromising legal or regulatory compliance. Digital and IT (inc cyber security and IT-related risks) form part of the Statement.

4.3.2 Within the parameters set by its Risk Tolerance, the University will manage IT-related risk by undertaking activities which support the fulfilment of its objectives and protection of institutional assets and intellectual property.

4.3.3 M[(4)]TJETQ0.000008 1 0 59.32 841.9 reW*nBT/F2 10.9 Tf1 0 0 1 113.6 248 Tm]TJc1GB

4.4.1 An IT Security Risk Assessment (RA Form) shall be completed by a member of the IT Services' Cyber Security Team:

Whenever a cyber threat is discovered that is recorded as a Priority 1 classification in the University's IT Service Management (ITSM) solution,

As part of the Service Transition to go-live for a new technical solution – particularly with a web-facing element - that may affect the cyber security defences of the University or hold Sensitive[7] data,

Bi-annually (every two years) following external penetration testing,

Whenever recommended by the Change Advisory Board upon consideration of a formal change request, or

When there are changes to cyber security standards to which the University requires, or aspires to gain, certification, e.g. Cyber Essentials+.

4.4.2 The results of IT Security Risk Assessments may be recorded in the University Risk Management Platform (RAP) through the creation of a new (or updated) risk entry within the divisional risk register, or institutional risk register if deemed significant enough to warrant escalation. The ITLT review the RAP platform every month so they will consider entry of new risks as part of the process.

4.4.3 Where action is required as a follow up to the IT Security Risk Assessment, this will be owned by the most relevant member of the IT Leadership Team, e.g. an infrastructure risk will be owner by the Assistant Director Infrastructure. They will resolve all remediatory actions and update the RAP as necessary until the associated risk entry can be closed or all outstanding mitigating actions have been resolved.

4.5

4.5.1 Information security risks are managed in line with the University's Risk Management Framework. It outlines each step of the risk lifecycle, including how risks are identified, assessed, treated, monitored, reviewed and reported.

4.6

4.6.1 Information Security Risk Assessments shall be completed with an understanding of:

Principles outlined in the Information Security Policy (ISP01);

The University's Statement of Risk Tolerance and Appetite

The University's Risk Management Framework

[7]