POLICY
Information Services

The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

# Information Security Policy 2015/16

## Contents

# 1. Introduction

Information is a vital and valuable product of the University's teaching, research and business activities. *Information Systems* are now a critical resource in enabling these core activities and communicating our work with our staff, students, alumni and business partners.

The University recognises that global access to information provides many opportunities but also many challenges. The commercialisation and ubiquity of the internet has allowed hackers, virus writers and professional criminal gangs to attack free and open academic networks. We are now dependent on a secure environment to undertake our core business and protection of our *information systems* and information assets is essential. The information security policy is built into the University's management of risk framework at the highest level. It applies to all members of the University and those who use University *information systems*.

## 1.1. Objective

The aim of the policy is to protect the University from security problems with its *information systems* and the information stored on them that might have an adverse impact on its operations, infrastructure or reputation. A secondary aim of the policy is to raise awareness of information security issues for all members of the University.

## 1.2. Principles

### 1.2.1. Scope

Information security shall include protection of the following:

- *Confidentiality*: Ensuring that information and systems are accessible only to authorised users.
- *Integrity:* Safeguarding the accuracy and completeness of information and processing methods.
- *Availability:* Ensuring that authorised users have access to information and systems when required.

This policy shall apply to:

- All *information systems* (including *computer equipment*, *network equipment* and telecommunications equipment) owned or operated by the University or *connected to the University network* by third parties.
- All software (including operating systems, network services and application software) installed on applicable *information systems*.
- All information stored on applicable *information systems*.

### 1.2.2. Approach

- The University will use all reasonable, appropriate, practical, and cost-effective measures to protect its *information systems* and achieve its security objectives.
- ISO 27001/BS7799: Information Security Management will be used as a guide for determining policy and managing security.

- The policy will comply with all legal and contractual requirements including but not limited to the **Regulation of Investigatory Powers Act (2000)**, the **Data Protection Act (1998)**, the **Human Rights Act (1998)**, the **Computer Misuse Act (1990), the Digital Economy Act (2010)** and the **JANET Acceptable Use Policy**.
- The policy should be read in conjunction with the **Code of Practice for Users of the University Computing Facilities**.
- The policy will not unnecessarily limit academic or individual freedom.

### 1.2.3. Responsibilities

- All *users* of University *information systems* are responsible for protecting information assets. *Users* must at all times act in a responsible, professional, ethical and security conscious way, maintaining an awareness of and conformance with the security policy.
- The University Executive Board (through the Chief Financial Officer) is ultimately responsible and accountable for ensuring that the objectives of the security policy are met.
- The Chief Information Officer is responsible for implementation of the policy and is authorised to pursue activities to achieve the policy objectives.
- Information Services is responsible for advising *users* on security issues, preventative monitoring of *information systems* and investigating security incidents.
- *Users* should report any breach in information security or suspected breach to the IT Service Desk (email: itservicedesk@nottingham.ac.uk), in accordance with the **Data Security Breach Incident Management Policy.**
- Information security best practice and the terms of this policy *shall* be considered at all points in the lifecycle of equipment, software and services developed by, specified by or procured by the University.

### 1.2.4. Practices

Further detailed policies will be produced to document specific areas of security policy. A list of the current detailed policies is provided in appendix A. Supporting standards and guidelines will also be produced to provide technical information on how to implement policies for specific platforms and environments. Standards are obligatory security measures to be followed at all times. Guidelines are recommended security measures to be followed when practical to do so.

The information security policy will be reviewed annually to determine whether it still meets the evolving needs of the information infrastructure.

### 1.2.5. Awareness

Information Services will publicise the policy, standards and guidelines to all members of the University. Information on known vulnerabilities and patches will be made available to *information systems users* and *administrators*. Information security awareness will be provided through seminars, training courses and published documents.

### 1.2.6. Applicability and Enforcement

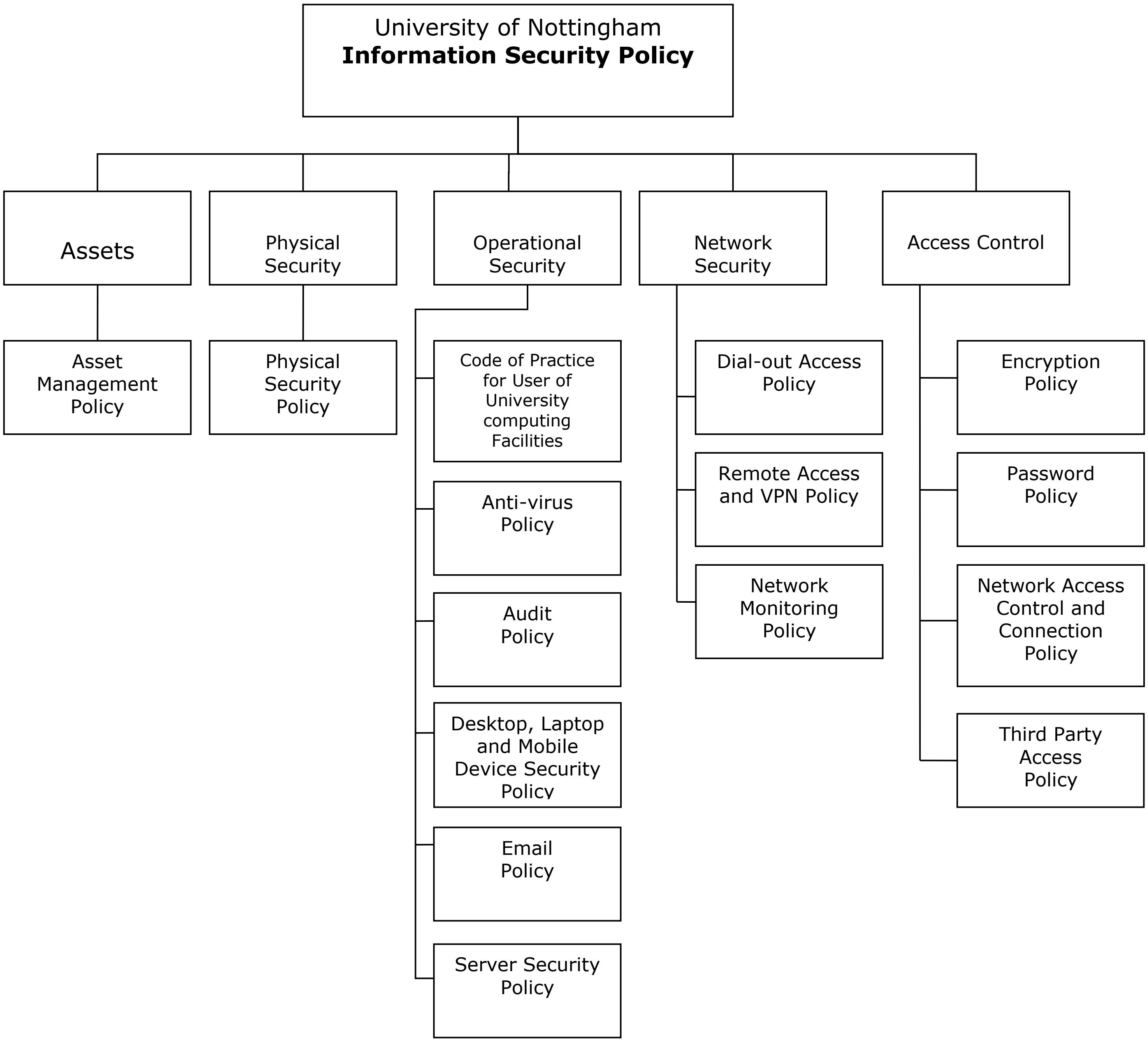
Information Services staff will monitor *information systems* and the network to detect unauthorised activity, identify potential weaknesses and pro-actively prevent security incidents.

This policy and compliance with it applies to all members of the University and those who use University *information systems*. Appropriate disciplinary action under the Code of Practice for Users of the University Computing Facilities *may* be taken against anyone disregarding the policy.

### 1.2.7. Exceptions

Exceptions to this Security Policy *may* be made at the discretion of the Chief Information Officer (CIO) or designee, or University Executive Board (UEB), subject to the level of additional risk to the network that may arise.

## 1.3. Appendix A: Detailed Policies



## 1.4. Appendix B: Explanation of Terms

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given elsewhere can be found here.

### 1.4.1. Keywords – Shall, Must, May

The keywords *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *may*, and *optional* in this document are to be interpreted as follows:

- ***Must***: this word, or the terms ***required*** or ***shall***, means that the definition is an absolute requirement of the specification.
- ***Must not****:* this phrase, or the phrase ***shall not***, means that the definition is an absolute prohibition of the specification.
- ***Should****:* this word, or the adjective ***recommended***, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- ***Should not****:* this phrase, or the phrase ***not recommended***, means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- ***May****:* this word, or the adjective ***optional***, means that an item is truly optional.

### 1.4.2. Other terms and definitions

The terms and definitions below have the given meaning throughout these policies. Any other computer-specific terms not included here shall be deemed to have the generally accepted computer industry definition given by **The Dictionary of Computer and Internet Terms** (Downing et al) or **Webopedia** (www.webopedia.com).

| **Term** | **Definition** |
|---|---|
| Administrator | Any University member or other person who is authorised to maintain or administer IT equipment. This would normally be *departmental* IT staff, Information Services staff or knowledgeable *users*. |
| Computer equipment | Any server, workstation, personal computer or laptop. |
| Connected to the University network | Either locally or remotely connected to the University network (as defined below). |
| Department, departmental | Refers to any School, department, division or other organisational unit of the University. |
| Mobile device | Any personal digital assistant, network-enabled mobile telephone or other small footprint device. |
| Information system | Any mechanism or method for storing information including but not limited to IT equipment. |
| Information Technology (IT) | Any *computer equipment* or technological process for storing information. |

| | |
|---|---|
| IT equipment | Any computer equipment, network equipment, telecommunications equipment or handheld device. |
| Laptop | A portable personal computer. |
| Locally connected to the University network | Connected to the University network via (a) a network access point from a University owned or operated building or (b) via a wireless connection to a wireless network access point operating from a University owned or operated building. |
| Network equipment | Any hub, switch, router or other equipment used to transport data across a network. |
| Personal Computer (PC) | A small single-user computer based on a microprocessor. |
| Personal Data | Data that relates to a living individual that can be identified from that data, or data that when combined with other information that is in the possession of or likely to come into the possession of the data controller that can identify a living individual. |
| Remotely connected to the University network | Connected to the University network via a modem, ISDN terminal adaptor, broadband modem, cable modem or other communications device through a dial-up access facility or an internet account operated by an Internet Service Provider (ISP). |
| Responsible user | A user who normally operates a specific piece of IT equipment. |
| Server | A multi-user computer offering services over a network. |
| Single-user computer equipment | Any personal computer, workstation or laptop that is used by a single person at a time and does not provide significant services to other network users. |
| (the) University campus | Refers to any campus or other accommodation occupied by *departments* of the University. |
| User | Any University member or other person who is authorised to use IT equipment. |
| Workstation | A powerful single-user computer with high quality graphics. |

### 1.4.3. Acknowledgement

This appendix is based on RFC2119 (S. Bradner 1997) and acknowledgement is hereby given.

# 2. Anti-Virus Policy

## 2.1. Purpose

To establish the requirements for effective virus detection and prevention

## 2.2. Scope

This policy applies to:

- All University owned or operated *computer equipment connected to the University Network*
- All Third-Party *computer equipment connected to the University Network*
- All *users* or *administrators* of the above *computer equipment*.

## 2.3. Policy

### 2.3.1. Use of Anti-Virus software

All *computer equipment* identified by the scope of the policy *shall* have anti-virus software installed and operational. On first installation of the anti-virus software a full virus scan of all attached storage devices (hard disks) *must* be completed.

### 2.3.2. Operation for workstations, Personal Computers and laptops

For *workstations, Personal Computers* and *laptops*, if the anti-virus software provides an 'always on' background process, this *must* be turned on. Regular, full virus scans *must* be undertaken.

Where the anti-virus software provides an automatic, scheduled virus scanning capability, this *must* be turned on. For *computer equipment* with 'always on' virus scanning, full virus scans *shall* be scheduled at least once a month. For *computer equipment* without 'always on' virus scanning, full virus scans *shall* be scheduled at least once a week.

Suspicious files received via email, network download, disk, CD or other media from unknown or untrusted sources *must* be scanned for viruses before being opened.

### 2.3.3. Operation for servers

For *servers*, if the anti-virus software provides an 'always on' background process, this *should* be turned on if this does not significantly affect the performance or operation of the *server*. Regular, full virus scans of the *server must* be undertaken at least once a month. Where a full virus scan affects performance or operation of the server, it is *recommended* that the scan be performed out of regular office hours, at weekends or during scheduled downtime.

Suspicious files found on the *server* or reported to the *server administrator* that come from an unknown or untrusted source *must* be scanned for viruses before being opened.

### 2.3.4. Updating virus signatures

Virus signature files *must* be updated regularly. Where the anti-virus software provides automatic checking for new virus signatures, this *must* be turned on. For *computer equipment* with automatic checking, the software *must* be scheduled to check for new virus signatures at least once a day. For *computer equipment* without automatic checking, manual checks *must* be made at least once a week.

### 2.3.5. Disinfecting Computers

Once a virus is detected the infected files *must* be disinfected, deleted or quarantined. If the file cannot be disinfected or removed automatically by the anti-virus software, the matter must be referred to the appropriate *administrator* or Information Services (itservicedesk@nottingham.ac.uk).

### 2.3.6. Creation or distribution of viruses

Any activities undertaken with the intention of creating and/or distributing viruses or other malicious code are prohibited, in accordance with the **Code of Practice for Users of the University Computing Facilities**.

### 2.3.7. Exceptions

Exceptions to this policy *shall* only be made in the following circumstances:

- No anti-virus software is available for the particular platform.
- All available anti-virus software conflicts with essential services or applications running on the *computer equipment* causing the system to crash or become unusable.

### 2.3.8. Responsibilities

*Users shall* be responsible for ensuring that anti-virus software is installed and operating on all *workstations, personal computers* or *laptops* they have been personally allocated. *Users may* request assistance from *administrators* or Information Services (itservicedesk@nottingham.ac.uk) in implementing this policy.
*Administrators shall* be responsible for ensuring that anti-virus software is installed and operating on *servers* or shared *computer equipment*.

### 2.3.9. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

### 2.3.10. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

### 2.3.11. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 3. Asset Management Policy

## 3.1. Purpose

To define the hardware, software and information assets of the University and its members. To define the minimum requirements for managing these assets in a secure way.

## 3.2. Scope

This policy applies to all hardware, software and information assets as defined below.

All *IT equipment* owned or operated by the University are hardware assets of the University.

All commercial software owned or licensed by the University and all open source software operated by the University are software assets of the University.

The contents of all databases, electronic mailboxes, word processing documents, spreadsheets, web pages, data files, configurations files and other *information systems* created by University members in the course of their duties are *information assets* of the University or its members[1].

## 3.3. Policy

Information assets are the ultimate product of the use of hardware and software assets. The creation, manipulation and dissemination of information assets is the lifeblood of the University.

Information assets *shall* be protected by the secure installation, configuration and updating of *information systems*. Secure installation, configuration and updating of hardware and software assets *shall* be verified, in part, by asset management and tracking.

## 3.4. Hardware assets

Information Services *shall* maintain an inventory of all hardware assets connected to the University network. The following information *shall* be maintained as part of the inventory.

- *Department*
- Location
- Owner (or *administrator*)
- Media Access Code (MAC) address
- Internet Protocol (IP) address (if fixed)
- Hostname
- Domain name

[1] Note that this document is concerned only with the protection of information assets. Ownership of an information asset in this context implies only possession of the asset and does not infer any definition of copyright ownership or intellectual property ownership

## 3.5. Software assets

Information Services *shall* maintain an inventory of all centrally licensed or owned commercial software. The following information *should* be maintained as part of the inventory.

- Software product
- Version
- Number of licensed copies
- Number of installed copies
- Owners or locations of installed copies

Departments and other groups within the University *should* maintain an inventory of all commercial software licensed or owned by the department.

## 3.6. Information assets

Information assets *should* be assigned an information classification based on the sensitivity of the information they contain. The classification should be one of the following:

| Information Category | Description |
|---|---|
| Public | This category covers information intended for public consumption or that can be made public without any negative implications for the business activities or reputation of the University. |
| Internal | This category covers information regarding the day to day business and academic operations of the University and is intended primarily for staff or student use. Some of the information in this category may be relevant for external parties who work closely with the University (suppliers, business or research partners etc) but external recipients would be expected to limit access to the information. The information would not be considered as of interest to the general public and therefore not appropriate for full public access, although public release would not cause serious reputational damage to the University. |
| Confidential | This category covers information of a more sensitive nature for the business or academic operations of the University. The information represents the University’s basic intellectual capital and know-how. Access should be limited within the organisation to those people who “need to know” for the performance of their duties or studies. |
| Highly Confidential | This category covers highly sensitive information that if released will cause significant damage to the University’s business activities or reputation or lead to a breach of the data protection act or similar legislation. Access to this information should be very restricted and the number of people who “need to know” will be relatively small. |

If an information asset includes information from different categories, it should be classified as the most sensitive category,

Each information asset *shall* have an owner. By default the owner of information assets stored on *IT equipment shall* be the person responsible for the *user* account under which the asset is stored (i.e. the possessor of the asset). Where the assets of multiple owners are collected into a common data store not under the control of a single person (e.g. a database), a notional owner *should* be assigned. The notional owner *may* be a leader or nominated individual of the group collecting information assets into the common data store or an *administrator* for the data storage package. By default the notional owner *shall* be the data store *administrator*.

Owners or notional owners of information assets *should* classify the relative value of their assets. Risk analysis *should* be performed for all assets that are critical to the operation of the core functions of the University, departments or administrative units.

## 3.7. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 3.8. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

## 3.9. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 4. Audit Policy

## 4.1. Purpose

To provide the authority for IT staff to conduct security audits on *IT equipment* in order to investigate security breaches or ensure compliance with University policy or other legal or contractual requirements.

## 4.2. Scope

This policy applies to:

- All University owned or operated *IT equipment.*
- All third party *IT equipment* permanently or temporarily *connected to the University network*.
- All *user*s or *administrators* of the above *IT equipment*.

## 4.3. Policy

### 4.3.1. Reasons for audit

Audits *may* be conducted to:

- Investigate known or suspected security breaches.
- Monitor conformance with the **Information Security Policy** and other legal or contractual requirements.

### 4.3.2. Authorised personnel

The Chief Information Officer *may* authorise Information Services staff to conduct audits on any *IT equipment* within the scope of the policy. *Department* IT Managers *may* authorise IT staff to conduct audits on *department IT equipment*. Audits *must* be conducted by authorised IT staff. Auditors *may* request and *shall* expect assistance from *administrators* or *users* responsible for the *IT equipment* being audited.

### 4.3.3. Limits of audit

The audit *should* only investigate those aspects of *IT equipment* related to its security functions and its compliance with policies and legal or contractual requirements.

### 4.3.4. Types of audit

***Security breach audit***

Where the audit is required to investigate a known or suspected security breach, an inspection of the *IT equipment shall* be made to attempt to discover how it was compromised and what damage was caused. The *user* or *administrator shall* facilitate access to the system for the auditor and provide administration level access if requested. The auditor *may* request that the inspection be undertaken by the *administrator* or a suitably knowledgeable *user* under the supervision of the auditor if physical access or other circumstances dictate. Information collected by authorised network monitoring activities *may* also be used in conjunction with information collected during the audit to draw conclusions.

***Conformance audit***

Where the audit is required to show conformance with policy, the auditor *may* require that the *administrator* or *user* provide evidence that the *IT equipment* complies with policy. An inspection of the *IT equipment* is *not required* unless the evidence requested is not provided or inconclusive. Automated auditing tools *may* be used in place of manual audits to facilitate the audit process. Information collected by authorised network monitoring activities *may* also be used to confirm or contest the evidence provided.

### 4.3.5. Audit follow-up

A report *shall* be produced by the auditor describing the findings of the audit and the required actions, if any, to recover from a security breach or ensure compliance with policy. The *administrator* or *user* responsible for the *IT equipment shall* complete all required recovery actions at the earliest opportunity. Copies of audit reports for department *IT equipment shall* be provided to Information Services auditors if requested.

Compromised or non-compliant computers *may* be disconnected from the network or have their network access restricted if their continued connection is deemed to present a serious and significant threat to the security or normal operation of the network or other *IT equipment* connected to the network.

### 4.3.6. Special situations

Special situations can be considered as follows:

- Where an audit is instigated at the request of a law enforcement agency investigating a criminal matter.
- Where there is a suspicion that child pornography is involved.
- Where a normal audit uncovers a potential criminal matter including child pornography.

In the above special situations at least two auditors *must* be present during any inspection of *IT equipment* or during the examination of other information collected by authorised network monitoring. Detailed notes of the investigatory steps taken *must* be made and signed by both auditors on completion of the audit.

Where a normal audit uncovers a potential criminal matter or child pornography, the audit *must* be stopped immediately and the *IT equipment* quarantined if possible. The Chief Information Officer or a designated representative *must* be informed and the Police notified.

## 4.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 4.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

## 4.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 5. Desktop, Laptop and Mobile Device Security Policy

## 5.1. Purpose

To establish minimum security standards for the configuration of *personal computers, workstations, laptops, handheld devices, mobile devices* and other *single-user computer equipment*.

## 5.2. Scope

This policy applies to:

- All *single-user computer equipment* including *personal computers*, *workstations* and *laptops locally connected to the University network*.
- All *laptops, handheld devices* and other mobile *computer equipment* that is (from time to time) locally *connected to the University network*.
- All *laptops, handheld devices* and other mobile *computer equipment not connected to the University network* but containing University related business data.
- All *users* and *administrators* of the above equipment.

## 5.3. Policy

### 5.3.1. Ownership and administration

All *single-user computer equipment must* have a designated person responsible for information security issues. This *may* be a knowledgeable *user* or a *departmental* or Information Services *administrator*.

All *mobile computers must* have a designated person responsible for information security issues. This *may* be a knowledgeable *user* or a *departmental* or Information Services *administrator*.

*Responsible users* of *mobile devices* or *single-user computer equipment* must inform the designated person, an *administrator* or Information Services (itservicedesk@nottingham.ac.uk) of any known or suspected security-related problem with the *computer equipment*.

*Users must* keep abreast of security issues for the operating systems they are using. They *shall* be expected to keep up to date with security announcements made by Information Services via the web (www.nottingham.ac.uk/is) or via IT Representatives.

Users should be aware that mobile computers are at greater risk of exposure to security threats than fixed location computer equipment permanently connected to the University network. The reasons for this include:

- Maintaining the physical security of a mobile computer in-transit or at an off-campus location may be more difficult.
- Theft or loss of mobile computers is more likely, increasing the risk of unauthorized access to data stored on them.

- Mobile computers may be connected to home or third party networks that are less secure than the University network leading to higher risk of exposure to malicious attack.

*Computer equipment should* be located in secure areas as described in the **Physical Security Policy**.

### 5.3.2. Single-user computer equipment configuration requirements

- *Computer equipment shall* be configured with a currently supported version of the operating system. Currently supported means that the manufacturer provides security patches or critical updates that protect against new vulnerabilities and that the version has not been designated as 'end of life'.
- *Computer equipment shall* be configured with currently supported versions of software. Currently supported means that the manufacturer or developer provides security patches or critical updates that protect against new vulnerabilities in a timely manner.
- *Computer equipment shall* be configured to provide only the services and resources required by the *users*. Services and applications that are not required *must* be removed or disabled.
- Information, services or resources that are not intended for general public access *shall* be protected by access-control mechanisms (e.g. passwords). Access *shall* be restricted to authorized *users* only.
- If the *computer equipment* provides a security event logging mechanism, this mechanism *shall* be turned on to assist auditing.
- If the *computer equipment* provides other event logging capabilities, this mechanism *should* be turned on to assist with problem diagnosis.
- Security patches *must* be installed on the system as soon as they are available. If an automated facility to check for patches and updates is available it *should* be used. The only exception to immediate patching is when this would adversely affect an application or service in use by a *user*.
- If a security patch cannot be applied within seven days of release, Information Services (itservicedesk@nottingham.ac.uk) *shall* be informed so that alternative security arrangements can be investigated.
- Anti-virus software *shall* be used as described in the **Anti-Virus Policy**.
- Services *shall* be run from non-privileged rather than administrator accounts where it is feasible to do so.
- Network communications that involve the transmission of passwords, authentication secrets, *confidential* or *highly confidential* information as defined in the **Asset Management Policy** *must* be encrypted, if a suitable encryption mechanism is available.

### 5.3.3. Mobile usage requirements

The University does not require staff to store or access confidential information using computing devices that it does not own or manage. Should the University require one of its members to use a mobile or home computing device to store or access confidential data, a suitably configured University owned device *shall* be provided.

Mobile computers are subject to the same general requirements as fixed location personal computers and *users must* follow the requirements of the **Personal Computer Security Policy**.

Access control mechanisms (e.g. passwords, PINs) *must* be used at all times to prevent unauthorized access to mobile computers. If the access control mechanisms are equipped with time-out protection such as automatic log-out or password protected screen locking, these *shall* be implemented. Where possible these *may* be implemented through administrative policies.

Personal firewalls provided as part of the operating system or a security suite *shall* be turned on and configured to allow only required Information Services.

Mobile communication services such as wireless networking, bluetooth or infrared *should* be disabled when not in use.

Disk encryption *must* be used to protect *highly confidential* University data as defined in the **Asset Management Policy**.

*Mobile computers should* be located in secure areas, as described in the **Physical Security Policy**, whenever possible. Physical security devices, such as laptop cable locks, *should* be used to protect mobile computers from theft when outside of secure areas.

*University owned mobile devices may* be remotely wiped following report of loss where this service capability exists to Administrators.

## 5.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Physical Security Policy**, **Anti-Virus Policy, Remote Access Policy** and **Encryption Policy**.

## 5.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

A *mobile computer* is a *laptop*, *mobile phone, handheld device* or other item of easily moveable *computer equipment*.

## 5.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 6. Dial-out Access Policy

## 6.1. Purpose

To identify the exceptional cases where dial-out access from the University campus is acceptable

## 6.2. Scope

Dial-out policy requirements apply to:

- All *users* of University owned or operated *computer equipment* that has a modem (internal or external) or an alternative telecommunication capability such as ISDN, ADSL or broadband that is not operated as part of the core University network by Information Services.
- All *users* of third party *computer equipment locally connected to the University network* that has a modem (internal or external) or an alternative telecommunication capability such as ISDN, ADSL or broadband that is not operated as part of the core University network by Information Services.

## 6.3. Policy

### 6.3.1. General obligations

A dial-out service allows *users* to connect directly to other networks and telecommunication services without using University network services (e.g. mail relays, web caches) and without passing through the University network gateways. Note that the definition of dial-out access in this context does not include internet-enabled mobile telephones, PDAs or other mobile devices unless they are also used to *connect locally to the University network*.

Dial-out access is extremely dangerous as it by-passes all the checks and safeguards (e.g. firewalls, virus checkers) provided for the University network. It provides a two way channel that may allow malicious code or individuals to gain access to the University network unseen and unchallenged.

Dial-out access *users must* follow the requirements and recommendations of the **Code of Practice for Users of the University Computing Facilities***,* the **Anti-Virus Policy** and the **Password Policy***.*

### 6.3.2. Service requirements

Dial-out access from *the University campus* via a modem, IDSN, ADSL, broadband or any other telecommunications service *shall not* be permitted, except by special waiver from the Chief Information Officer or a designated representative.

A special waiver *shall* be granted only where the connectivity required cannot be achieved via the normal University network services and where there is a legitimate business or academic reason for it.

*IT equipment* granted a special waiver and allowed dial-out access *shall* be registered with Information Services.

All *IT equipment* permanently connected to the University network without a dial-out waiver but with a dial-out capability, whether enabled or not, *shall* be registered with Information Services.

*IT equipment* permitted dial-out access *shall* be configured with a firewall. The firewall *shall* be configured to allow only the services required in support of the dial-out access.

*IT equipment* permitted dial-out access *shall* be installed with anti-virus software and comply with the requirements and recommendations of the **Anti-Virus Policy**.

*IT equipment* permitted dial-out access *should* be disconnected from the University network either permanently or temporarily while dial-out is active, unless this interferes with its normal operation.

## 6.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 6.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

## 6.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 7. Email Policy

## 7.1. Purpose

To establish the requirements for safe use of electronic mail (email).

## 7.2. Scope

This policy applies to all *users* who send or receive email via the University network or from University email systems, whether accessed from on or off campus.

## 7.3. Policy

### 7.3.1. Information Services responsibilities

All email entering or leaving the University network *shall* pass through the email filtering service and mail relays operated by Information Services or designated third parties. This includes email passing to or from *departmental* or group mail relays. Email travelling entirely within the University network is *not required* to pass through the email filtering service.

The email filtering service *shall* provide automated scanning of email to detect potential *malicious code* and to identify *spam*.

*Malicious code* signatures, *spam* identification rules, blacklists and other mechanisms required by email scanning tools to identify new or modified threats *shall* be kept up to date. Checks for updates *shall* be performed at least once a day.

***Detection of malicious code***
Email items or attachments identified as containing *malicious code* or suspected of containing *malicious code shall* be prevented from reaching the intended recipient. The intended recipient of an infected or suspected email *should* be informed that the email did not reach its destination.

***Identification of spam***
Email items identified as *spam* or suspected of being *spam shall*, where possible, be quarantined before reaching the intended recipient's mail client. Quarantined email items shall be reported to the intended recipient at regular intervals so that they may confirm the items have been classified correctly. Incorrectly quarantined email items *shall* be released to the intended recipient when requested.

### 7.3.2. Email *user* responsibilities

*Malicious code* is developed and released on a regular basis. *Users must* remain vigilant for new threats which automated scanning tools may not yet be able to detect.

*Users must not* create or modify *malicious code* (unless as part of a legitimate and authorised academic course or research project and under the supervision of a member of staff experienced in this field).

*Users must not* knowingly send *malicious code* through the email system or otherwise allow it onto the University network by other means.

*Users must not* send, forward or otherwise distribute *spam* or chain letters.

Email attachments from unknown sources *must* be scanned for *malicious code* before being opened.

Since some *malicious code* can fake the sender of an email, messages from known senders that are unexpected or in any way unusual *should* be scanned for *malicious code* before being opened.

Staff *must not* configure their University email accounts to automatically forward email to services not operated by the University.

*Users* conducting University business or communications via email *must* use a University provided email account. Personal email accounts *must not* be used for conducting University business or communications.

***Phishing***

*Phishing* is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or Information Services are commonly used to lure the unsuspecting. *Phishing* is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Information Services will never request password information via email or telephone and any such request should be reported.

## 7.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy, Password Policy,** and **HR Policy for Electronic Mail Usage**.

Further information on *phishing* can be found at the Anti-Phishing Working Group (APWG) http://apwg.org/consumer_recs.html

## 7.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

*Malicious code* is defined as any executable, script, macro or other programmable feature that has the potential to damage, control or otherwise compromise the security of a *user's* computer. This includes viruses, trojans, worms and spyware.

*Spam* is defined as indiscriminate, unsolicited, bulk commercial email. It is often about subject matter that is of no interest, or offensive, to the intended recipient.

*Phishing* is a targeted email that requests information such as usernames and passwords from the *user* purporting to come from a source of authority.

## 7.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 8. Encryption Policy

## 8.1. Purpose

To define the minimum requirements for the safe encryption of data

## 8.2. Scope

This policy applies to all *users* of University *IT equipment*.

## 8.3. Policy

Encryption is the process of disguising data so as to hide its substance from any casual observer gaining access to it. This is done by applying a mathematical function, known as a *cryptographic algorithm* or *cipher*, to the data to render it unreadable. A mathematical function that reverses the encryption process is used to decrypt the data. One or more unique *keys* is used in conjunction with the *cipher* to perform the encryption or decryption.

### 8.3.1. General

- Data that is classified as *confidential,* as defined in the **Asset Management Policy**, *should* be encrypted.
- Data that is classified as *highly confidential*, as defined in the **Asset Management Policy**, *shall* be encrypted.
- Data requiring an integrity guarantee *should* be encrypted.
- *Users* requiring strong authentication of a person, service or data item *should* use encryption as part of the authentication technique.

### 8.3.2. Encryption strength

Only tools and products based on proven, mathematically sound *cryptographic algorithms*, subjected to peer review by the cryptographic community, *shall* be used for encryption.

For block ciphers, a minimum symmetric key length of 128 bits *should* be used. For long term security a symmetric key length of 256 bits is *recommended*. For public key ciphers, a minimum asymmetric key length of 2048 bits *should* be used. For long term security an asymmetric key length of 4096 bits is *recommended*.

All keys *shall* be stored safely. Where a key is secured by use of a *pass phrase*, the *pass phrase shall* be at least 12 characters in length.
The requirements and recommendations for password selection and password protection described in the **Password Policy** *shall* apply for *pass phrases*.

### 8.3.3. Ciphers and products

The following ciphers are *recommended* for use on University *IT equipment*.

- *Block Ciphers*: 3DES, IDEA, RC5, AES, CAST, Blowfish
- *Public Key Ciphers*: RSA, Diffie-Hellman
- *Hash Functions*: MD5, SHA

The following products are *recommended* for use on University IT equipment.

- Remote Access: SSH, IPSec, L2TP and PPTP VPNs.
- Web Security: SSL
- Email: Pretty Good Privacy (PGP), TLS, Authenticated SMTP
- File Security: PGPDisk

Note that some of the above ciphers and products contain patented algorithms or methods which may require the purchase of a suitable licence.

## 8.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 8.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

- A *cryptographic algorithm* or *cipher* is a mathematical function applied to data to make it unreadable to a casual observer.
- A *block cipher* is a cipher that is applied to a block of data (a number of characters or bits) at the same time. This is different from older ciphers which are applied to a single character at a time.
- A *public key cipher* is a cipher that uses different keys for encryption and decryption. A public key is used for encryption and a private key is used for decryption. The public key cannot be used to decrypt the data and so can be freely published or given to correspondents that need to send you confidential data.
- A *hash function* is a cipher that produces a unique sequence of characters or numbers (the hash) for any different collection of input data. A hash function can be used to verify that the data has not changed since the hash was generated.
- A *key* is a sequence of characters or numbers, like a password, that is used with a cipher to encrypt or decrypt data.
- A *pass phrase* is a sequence of characters or numbers, like a password, that is often used to gain access to a stored key.

## 8.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 9. Network Monitoring Policy

## 9.1. Purpose

To establish the requirements for monitoring, logging and retention of traffic on the University network.

## 9.2. Scope

This policy applies to:

- All *IT equipment locally connected to the University network.*
- All *IT equipment remotely connected to the University network* whilst the equipment is connected to the University network.
- All *users* of the above equipment.

*Users* should also be aware that the **Audit Policy** allows for the auditing of *IT equipment* to investigate security breaches and monitor compliance with policy.

## 9.3. Policy

The ***Regulation of Investigatory Powers Act (2000)*** allows authorised Information Services staff to monitor network traffic for operational and security reasons.

Specifically, Information Services *may* intercept network traffic without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime, gross misconduct or unauthorised use, and ensuring the efficient operation of University communications systems.

The primary aims of network monitoring are:

- To maintain the integrity and security of the University network, *IT equipment* and information assets.
- To collect information to be used in network design, engineering, trouble-shooting and usage-based accounting.

## 9.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy,** and the **Audit Policy.** This policy complies with the requirements of the ***Regulation of Investigatory Powers Act (2000)***.

## 9.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

## 9.6. Enforcement

Any *user* found to have violated this policy *may* be subject to disciplinary action.

# 10. Network Access Control and Connection Policy

## 10.1. Purpose

To establish the requirements and operational principles for the management of network traffic crossing the boundary between a) the University network and b) JANET and the Internet. To establish the requirements for connection of *IT equipment* to the University network.

## 10.2. Scope

This policy covers all *IT equipment locally connected to the University network and* all network traffic passing between the University network and other networks including JANET and the Internet.

*Computer equipment remotely connected to the University network* is covered by the **Remote Access and Virtual Private Networking Policy**.

## 10.3. Policy

### 10.3.1. University Network

The University network consists of a wired network accessed via plug-in data points in University buildings and a wireless network accessed via broadcasts from wireless access points around the campus. The University network is operated by Information Services.

*Computer equipment* is attached to the wired network by connection to a plug-in data point using a compatible network cable. *Computer equipment* with a wireless capability is joined to the network by connecting via a wireless access point using the secure network identifier (SSID: UoN-secure) and authenticating using a University username and password.

*IT equipment must* maintain a hardware address that uniquely identifies it University-wide. For most IT equipment the hardware address will be the Media Access Code (MAC) address associated with the network card.

All University-owned *IT equipment* to be connected to the wired network *must* be registered with Information Services prior to connection.

Each connection to the University network *shall* provide access for a single computer or mobile device. Multiple computers or mobile devices *shall not* be connected though a single wired or wireless network connection. Multiple devices connected through a single network connection *may* be disconnected from the University network.

Personal laptops and mobile devices *may* be connected to the wireless network but *shall not* be connected the wired network except in libraries and computing rooms operated by Information Services where labelled laptop plug-in points are provided.

*Users must not* change the hardware address associated with an item of *computer equipment* connected to the wired network, or replace or swap a NIC without first registering the change with Information Services.

All *network equipment* forming the University network shall be owned and managed by Information Services.

Personal *network equipment,* including wireless access points, *shall not* be connected to the University network.

*Network equipment,* including wireless access points, owned by schools or professional services departments *shall not* be connected to the University network except in exceptional circumstances and with prior, written authorisation from the Chief Information Officer (CIO) or designee.

Computers or mobile devices with the capability to act as wireless access points or network routing devices for other computers or mobile devices *shall not* be connected to the University network unless the wireless access point or network routing features are disabled.

Information Services *shall* supply network settings, including a hostname and IP address, and *shall* ensure that the equipment is configured correctly for network use.

*Users* connecting *IT equipment* to the University network *may* be required to install software to ensure compliance with the **Network Access Control and Connection Policy*.***

Where the *IT equipment* is in a fixed location, Information Services *may* provide a fixed IP address.

Where the *IT equipment* is expected to change locations or not be permanently connected to the network (e.g. a *portable computer*), Information Services *may* provide a dynamically allocated IP address.

*IT equipment* using a dynamic IP address *shall* use the Dynamic Host Configuration Protocol (DHCP) to automatically configure network settings.

*IT equipment* using a fixed IP address *should* use DHCP to automatically configure network settings.

*Users* must not, at any time:

- invent network settings or host identities;
- alter network settings or host identities;
- transfer network settings or host identities from one computer to another.

### 10.3.2. Connection

Network traffic passing between the University network and other networks *shall* be controlled by network access control mechanisms such as firewalls, intrusion detection systems, network address translators and virus checkers.

Network access control mechanisms *should* be placed at all inter-connection points of the University network with other networks. Network access control mechanisms *may* also be placed between subnets of the University network.

Information Services *shall* determine the network services required by *departments*, administrative units and other groups to facilitate the teaching, research and business activities of the University.

Information Services *shall* permit required network traffic that needs to communicate with other networks to pass through the network access control mechanisms, provided the security of the University network is not compromised.

Information Services *shall* prevent any network traffic from passing through the network access control mechanisms that compromises the security of the University network or any other network.

***Principle of least access***

All network traffic not specifically required to conduct University activities *shall* be denied by the network access control mechanisms. Network traffic *should not* bypass the network access controls by means of reverse connections or tunnelling over permitted protocols.

The triplet (source address, destination address, protocol or port) *should* be as specific as possible, consistent with any practical restrictions, when determining network access control rules.

***Inbound traffic***

New *inbound* traffic from untrusted sources *should* be terminated on servers in a DMZ. There *should* be no unapproved access from external networks to the internal networks. Existing internal servers directly accessible from outside the University network *should* be migrated to a DMZ.

The permitted *inbound* protocols *shall* be documented and *may* be published.

The following principles apply:

- *Inbound* HTTP and FTP calls *shall* be restricted to identified servers.
- All *inbound* SMTP (Mail) traffic *must* have a destination of one of the established University mail relay servers.
- DNS queries and zone transfers *shall* be restricted to identified University DNS servers.

***Outbound traffic***

In general *outbound* traffic is permitted from any host. Specific protocols *may* be restricted to named hosts or subnets and some protocols *may* be prohibited.

The permitted *outbound* protocols *shall* be documented and *may* be published.

The following principles apply:

All *outbound* HTTP traffic *should* go through one of the established web proxy servers.

### 10.3.3. Logging

Network access control systems *shall* log all denied traffic and *may* log all traffic originating from untrusted or less trusted networks, including Internet and extranet traffic that is destined to the University network. Logs *must* be maintained online for at least 7 days, and offline for at least 30 days.

### 10.3.4. Audit

Network access control system rules *must* be tracked and audited regularly to ensure that unneeded rules are removed. Any rule that is unused within 12 months *may* be removed unless it can be shown to be required.

### 10.3.5. Change request procedures

There *must* be an audit trail for every network access control configuration change made. Changes *must* be formally requested and approved by Information Services. Once the change is approved, records *must* be made of the changes and rollback procedures *must* be used.

### 10.3.6. Access Control

Logical or physical access to network access control systems *shall* be restricted to authorised personnel. Procedures to log both physical and logical access *should* be put into place.

## 10.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy** and the **Network Monitoring Policy.**

## 10.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

*Inbound* is defined as initiated from outside of the University network.
*Outbound* is defined as initiated from inside of the University network.

## 10.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action, possibly including loss of network access privileges.

# 11. Password Policy

## 11.1. Purpose

To establish minimum standards for password selection and use.

## 11.2. Scope

This policy applies to all *users* of University *IT equipment*.

## 11.3. Policy

### 11.3.1. General

All *IT equipment* that supports an access control mechanism based on user accounts and passwords or PINs *shall* have the mechanism enabled.

User accounts *must* have a password or PIN set.

Passwords *must* contain at least seven characters. It is *recommended* however that passwords contain at least twelve characters to reduce the chance of compromise by a brute-force password-cracking attack.

Passwords *shall* contain a combination of numbers, and upper and lower case letters.

If the access control mechanism allows it, a password *should* contain at least one special character (e.g. underscore, dollar, ampersand).

Passwords *must not* be words found in a dictionary, personal information that can be associated with the owner (e.g. birthdays, telephone numbers) or simple patterns (e.g. abc123).

The *recommended* process for choosing a password is:

- Think of a memorable phrase on which to base the password.
- Replace words by meaningful numbers or special symbols (e.g. to, too = 2, for = 4, and = &, money, cash = £).
- Use the first letters of the remaining words in the phrase.
- Capitalise some of the first letters.
- Replace letters by numbers or special characters that look similar (e.g. I = 1, o = 0, s = 5 or $).

e.g. aSLi4Lnj4C = a student loan is for life not just for Christmas
IoHw1DR! = I'm only happy when I'm doing research!
Tl0£iTr0aE = The love of Money is the root of all evil

Passwords for staff, postgraduate research students and users with an associate IT account *must* be changed every 180 days.

### 11.3.2. Multiple accounts

*Users* with multiple user accounts for different services or multiple computers *should* set a different password for each account. *Users should not* use the same passwords for University and non-University user accounts. This will limit the damage should any one user account be compromised.

### 11.3.3. User password protection

*Users must not* reveal their own passwords to anyone including IT staff or system administrators. If IT staff require access to your user account they will be able to accomplish this through an *administrator* account or by changing your password.

All passwords *must* be treated as sensitive, confidential University information.
If someone demands a password, refer him or her to this document or have them contact Information Services (itservicedesk@nottingham.ac.uk).

*Users must not* use the "Remember Password" feature of any operating system or application.

*Users must not* store passwords in a file on any computer without encryption.
*Users must not* write down or store passwords in any location easily accessible to others.

### 11.3.4. System password protection

*IT equipment* access control mechanisms *shall* enforce the password length, password complexity and password change requirements detailed in section 3.1 to ensure *user* compliance.

In addition, *IT equipment* access control mechanisms *shall* further limit the risk of password compromise by enabling the following features where available:

- Password History Control: The access control mechanism *must* prevent the reuse of a *user's* last eight passwords.
- Account Lockout: The access control mechanism *shall* prevent any further logins after three failed login attempts. The lockout *should* be for a fixed period of time or until the account is reset.
- Concurrent Connections: The access control mechanism *shall* prevent an excessive number of concurrent connections by the same *user* above and beyond those reasonably required to access authorised and necessary *Information Systems*.
- Grace Logins: The access control mechanism *should* allow the *user* seven login opportunities to change their password when the password age limit is reached after which the account *should* be locked.

## 11.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy, Identity and Access Management Policy** and **Email Policy**.

## 11.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

## 11.6. Enforcement

Any *user* found to have violated this policy *may* be subject to disciplinary action.

# 12. Physical Security Policy

## 12.1. Purpose

To establish the requirements for physical security of *information systems.*

## 12.2. Scope

This policy applies to:

- All University owned or operated *information systems*.
- All *third party IT equipment locally connected to the University network*.

## 12.3. Policy

### 12.3.1. Location of Information Systems

*Information systems should* be housed in a secure area protected by a defined security perimeter with entry controls. *Servers shall be* located within recognised Information Services data centres.

***Secure areas***
A secure area *shall* be a room or building with a clearly defined security perimeter. The security perimeter, usually the walls, windows and doors of the room or building, *shall* act as a physical barrier between the secure area and any unsecured areas preventing access except through designated entry control points. The security perimeter *should* be physically sound to prevent possible break-in.

***Entry controls***
An entry control *shall* be a mechanism for limiting access to a secure area to authorised personnel only. An entry control *may* be a lockable door, a smart card entry system or a staffed reception area.

### 12.3.2. Access to IT equipment

Entry control mechanisms *should* be enforced at all times when *IT equipment* is left unattended. Where *IT equipment* is left unattended for significant periods (e.g. overnight or at weekends), additional security measures such as door or window alarms or motion detectors *may* be used.

Unauthorized personnel *should* be permitted into secure areas only when accompanied by authorised personnel.

### 12.3.3. Protection of IT equipment

Secure areas *shall* be operated and maintained so as to minimize the risk from theft, fire, explosion, smoke, water, dust, vibration, chemical effects, electrical supply interference or radiation.

***Backups***
*IT equipment* containing critical or important information assets *shall* have those assets backed according to the **Backup Policy**.

***Power supply***
*IT equipment* performing critical services or containing critical information assets *should* be fitted with an uninterruptible power supply to allow continued operation or controlled shutdown in the event of electrical supply interruption.

***Maintenance***
*IT equipment should* be maintained in accordance with the supplier's recommended service intervals and specifications.

## 12.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy** and **Backup Policy**.

## 12.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

## 12.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

# 13. Remote Access and Virtual Private Network Policy

## 13.1. Purpose

To establish the requirements for safe use of remote connections to the University network from off campus.

## 13.2. Scope

This policy applies to:

- Remote access policy requirements apply to all *users remotely connecting to the University network* from off campus.
- All *users* employing VPN technology to *remotely connect to the University network* from off-campus locations via the Information Services supported VPN gateway.
- All *users* requiring a VPN connection from the University network, through the firewall, to a VPN terminator outside the University network and operated by a third party.
- IT staff configuring VPN connections between campus locations.

Remote access implementations covered by this policy include, but are not limited to, dial-in modems, ISDN, ADSL and cable modems which provide narrowband or broadband access to the University network via the Internet.

## 13.3. Policy

### 13.3.1. General

Remote access *users* should note that by connecting to the University they become part of the University network and *must* treat any computer connected in this way as if it were on *the University campus*. In particular they *must* follow the requirements and recommendations of the **Code of Practice for Users of the University Computing Facilities***,* the **Anti-Virus Policy**, the **Password Policy** and the **Email Policy***. Users* should also follow the requirements of the **Mobile Computing Policy** or **Personal Computer Security Policy** as appropriate. If remote access is used to connect to the internet via the JANET gateway, the requirements of the **JANET Acceptable Use Policy** *must* also be followed.

### 13.3.2. Service requirements

Remote access allows *users* to connect to the University network from an internet account provided by an Internet Service Provider (ISP) or third party network provider. The operation and maintenance of an internet account is a matter for the user and their ISP. The University plays no part in provision of the service. Remote access to the University network *shall* be made over a secure, encrypted connection whenever this is available. Acceptable secure communication services include VPN, secure sockets layer (SSL), secure shell (SSH) and remote desktop. Insecure communications services *shall* be restricted but *may* be allowed in exceptional circumstances.

Access to services that do not provide a secure, encrypted connection *should* be tunnelled through a secure connection whenever possible. It is *recommended* that a Virtual Private Network (VPN) be used if one is available.

*Users shall* only attempt to connect to computers or services on the University network for which they are authorised.

Connections from remote locations *shall* be logged and *may* be monitored as described in the **Network Monitoring Policy**.
Remote access to the University network is provided to allow University members to perform legitimate academic or administrative activities in conjunction with their work. Use of the connection *shall* be limited to authorised *users* only. The facility *must not* be used by family members, housemates or other persons at the off campus location.

***Remote Access Gateway***
Where available, *users should* connect to the University network through use of a Remote Access Gateway rather than directly.

### 13.3.3. Third-party remote access

Remote access for third parties, such as vendors, *shall* be granted only for legitimate business reasons (e.g. as part of a support contract for Information Services or equipment).

All third parties requiring remote access *shall* be registered with Information Services.

Access for third parties *shall* be restricted to the *IT equipment* or services that they are providing. All remote connections *shall* be logged.

### 13.3.4. Incoming VPN service

Information Services provides a VPN capability that allows authorised *users* to create a VPN connection from their Internet Service Provider (ISP) internet accounts to the University network. The VPN allows access to IT services normally only available from within the campus network because:

- they cannot be provided securely across the internet or
- a University network IP address is a requirement to authenticate a *user* as a legitimate member of the University.

Security for otherwise insecure services is achieved by the VPN by encrypting all network traffic from the *user's* remote computer as it travels over the public internet connection.

The operation and maintenance of an internet account is a matter for the *user* and their ISP. The University plays no part in provision of this part of the service. It is also the *user's* responsibility to check that their ISP permits the use of VPN protocols as part of their service agreement.

Access to the University network *shall* be via a VPN gateway managed by Information Services.

All VPN connections *shall* terminate at the VPN gateway. This allows the traffic to be inspected by the University firewall and network monitoring tools.

The VPN service *shall* be limited to authorised *users* by means of tokens, certificates, public/private keys, passwords or other authentication mechanisms.

Users *shall* protect any token, certificate, key or password they are given from unauthorised access.

Users *must not* attempt to access any VPN service for which they are not authorized.

Users *must not* allow family members, housemates or other unauthorized users to gain access to the VPN service.

***Incoming VPN service levels***

Different types of VPN access providing different levels of service *may* be provided by Information Services. These *may* include SSL VPN connections and IPSec VPN connections. Where different levels of access are provided, Information Services *shall* assess which method a user requires based on their IT needs.

Information Services shall manage the IT services accessible through the VPN to ensure that any additional risk to the security of the campus network is minimised.

***IPSec VPN requirements***

For IPSec VPN usage, users *shall* employ:

- A VPN client supplied by Information Services; or
- An IPSec compliant VPN client approved by Information Services.

*Users shall* ensure that computers *remotely connected to the University network* via a VPN pass all network traffic through the VPN tunnel. Traffic for sites on the internet *shall* be passed through the VPN tunnel and then the JANET gateway or *shall* be dropped. Dual or split tunnelling allowing access to the University network via VPN and other internet sites via the *user's* ISP *shall not* be permitted as this provides a back-door for malicious code or users to enter the University network.

Users *shall* disconnect from the VPN gateway after thirty minutes of inactivity. Users *must not* use pings or other artificial network mechanisms to keep a connection open when not in use.

***SSL VPN requirements***

For SSL VPN usage, user *shall* employ:

- An industry standard, trusted and secure web browser.

### 13.3.5. Outgoing VPN connections

Outgoing IPSec VPN connections shall not be permitted (to comply with the **Network Access Control Policy** principle of least access), unless a significant benefit to the University can be shown.

Requests to operate an outgoing IPSec VPN connection shall be subject to **Network Access Control Policy** change request procedures and shall be reviewed by Information Services. The requestor shall be required to demonstrate that the security policy implemented at the VPN termination network is at least as rigorous as that at the University.

## 13.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy,** the **Code of Practice for Users of the University Computing Facilities***,* the **Mobile Computing Policy**, the **Personal Computer Security Policy**, the **Anti-Virus Policy**, the **Password Policy** and the **Email Policy**.

## 13.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

## 13.6. Enforcement

Any *user* found to have violated this policy *may* be subject to disciplinary action, possibly including loss of remote access privileges.

# 14. Server Security Policy

## 14.1. Purpose

To establish minimum security standards for the configuration of *servers*.

## 14.2. Scope

This policy applies to all *servers locally connected to the University network*.

## 14.3. Policy

### 14.3.1. Ownership and administration

*Servers* that provide a service available to *users* external to the University network *shall* be configured and maintained by qualified IT staff.

*Servers* that provide critical or University-wide services in support of teaching, research or business functions *shall* be configured and maintained by qualified IT staff.

*Server administrators must* keep abreast of security issues for the operating systems, services and applications they are maintaining. They *shall* be expected to subscribe to any freely available email or other service that provides them with timely information on security issues or patches.

*Servers shall* be located in secure areas as described in the **Physical Security Policy**. Where possible, servers *shall* be hosted within Information Services data centres.

### 14.3.2. Server configuration requirements

- *Servers* providing services to external *users* or providing critical services to internal users *shall* be configured with a recognised and generally accepted server operating system.
- *Servers shall* be configured with a currently supported version of the server operating system. Currently supported means that the manufacturer provides security patches or critical updates that protect against new vulnerabilities and that the version has not been designated as 'end of life'.
- *Servers shall* be configured with currently supported versions of software. Currently supported means that the manufacturer or developer provides security patches or critical updates that protect against new vulnerabilities in a timely manner.
- *Servers shall* be configured to provide only the services and resources for which they are intended. Services and applications that will not be required *must* be disabled.
- *Servers* that provide access to services, resources or information that is not intended for general public access *shall* be protected by access-control mechanisms (e.g. passwords, firewalls). Access *shall* be restricted to authorised *users* only.

- If a *server* or service provides a logging mechanism, access to the service *shall* be logged in accordance with the **Network Monitoring Policy**.
- Security patches *must* be installed on the system as soon as is practical. The only exception to this requirement is when immediate installation would interfere with business requirements or adversely affect the service being offered.
- If a security patch cannot be applied within seven days of release, Information Services (itservicedesk@nottingham.ac.uk) *shall* be informed so that alternative security arrangements can be investigated.
- Trust relationships between systems *shall* be avoided if other suitable authentication mechanisms are available.
- The principle of "least required access" *shall* be used to provide services and resources.
- Services *shall* be run from non-privileged rather than *administrator* accounts where it is feasible to do so.
- Network communications that involve the transmission of passwords, authentication secrets or restricted information *shall* be encrypted, if a suitable encryption mechanism is available.

## 14.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **IS Server Hosting Policy, Physical Security Policy** and the **Network Monitoring Policy**.

## 14.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in appendix B of the **Information Security Policy**.

A *server* is defined as a multi-user computer that provides a service (e.g. database access, file transfer, remote access) or resources (e.g. file space) over a network connection.

## 14.6. Enforcement

Any *administrator* or *user* found to have violated this policy *may* be subject to disciplinary action.

# 15. Third-Party access Policy

## 15.1. Purpose

To establish expectations for third parties and contractors about maintaining the security of University of Nottingham *information systems*.

## 15.2. Scope

This policy applies to all *third parties* working on *information systems* belonging to or provided for the University of Nottingham including *formally* or *informally outsourced services*. It also covers:

- Guest-access to University systems
- Third party support, maintenance & development

## 15.3. Policy

### 15.3.1. Risk

In the absence of control or accountability by the University, there is a degree of risk associated with entrusting information to third parties.

- Who may have access to the data
- How user data is used
- Where user data is stored
- Security of user data
- Availability in the short, medium & long term
- Whether user data is recoverable in the event of a disaster
- Availability of support in the event of a problem
- How the facility may change in terms of the user interface or nature of the service

### 15.3.2. Managing risks

Use of *informally outsourced* services to store sensitive or *personal data* may be in breach of the Data Protection Act.

*Informally outsourced* services *must not* be approved or promoted for handling confidential information.

An assessment of the potential impact to the University that could result from the *third party* suffering or causing a problem *should* be carried out.

European Union law requires that personal data *shall not* be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal data to be stored in China and Malaysia *shall* also adhere to local legislation regarding data protection

The *third party must* agree to follow the **University Information Security Policy.**

### 15.3.3. Guest access by third parties

Where *third parties* are providing support and maintenance of University *information systems* it may be necessary for them to access these systems at the highest level of privilege. It is essential that:

- All such privileged access to or via the University network is approved by Information Services
- A member of University staff is responsible for managing the access in terms of scope, level and duration. All access by *third parties should be* monitored or logged.
- Remote access to *information systems must* only be permitted via secure encrypted network protocols.
- The *third party should* provide the University with the code of practice that their staff or agents must follow when handling the customer's information. It is preferable that this code of practice forms part of the agreement with the *third party* for provision of service

University members *must not* permit information security safeguards and policies to be bypassed, or allow inappropriate levels of access to University *information systems*.

Any access to *information systems* provided to *third parties* must follow recognised procedures. For example use of IAM to provide Associate Accounts for access to computing services.

## 15.4. Related policies, standards and guidelines

This document should be read in conjunction with the University's **Code of Practice for use of computing facilities**, **Identity and Access Management Policy, Network Access and Connection Policy**, **Encryption Policy**, **Remote Access and Connection Policy**, **and Server Security Policy.**

## 15.5. Terms and definitions

*Third Parties* – external organisations or individuals other than the University's own staff or students.

*Informally outsourced services* – Services provided by a third party company for which there is no formal bilateral agreement or control over data. E.g. Gmail

*Formally outsourced services* – Services provided to the University by third parties and subject to a formal bilateral agreement or contract, with clear understandings setting out standards and expectations regarding information security.

## 15.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

Contracts and agreements with Third Parties *should* include means for redress by the University in the event of a dispute.