Acceptable Use Policy (AUP)

For this assignment, you need to find three examples of an AUP from the Internet or other sources. Download these or copy them and convert them into a PDF to attach to your submission. After reading/skimming these AUPs, attempt to write your own abbreviated AUP. Keep your AUP to a maximum of 5 pages and a minimum of 3 pages. You can cut and paste from your examples; however, be advised that this needs to fit the needs of the small marketing company from modules 5 and 6. Change text accordingly if you copy from other sources and make sure it is relevant.

Submit your paper and the 3 PDF examples for this assignment.

Small company’s name has been used as Small Comp.

Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of all (Small Comp’s) information and IT equipment. It also includes the use of email, internet, voice, and mobile IT equipment. This policy applies to all (Small Comp’s) employees, contractors, and agents (hereafter referred to as ‘individuals’).

This policy applies to all information, in whatever form, relating to (Small Comp’s) business activities worldwide, and to all information handled by (Small Comp) relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by (Small Comp) or on its behalf.

# Computer Access Control – Individual’s Responsibility

Access to the (Small Comp) IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the (Small Comp’s) IT systems.

**Individuals must not:**

* Allow anyone else to use their user ID/token and password on any (Small Comp) IT system.
* Leave their user accounts logged in at an unattended and unlocked computer.
* Use someone else’s user ID and password to access (Small Comp’s) IT systems.
* Leave their password unprotected (for example writing it down).
* Perform any unauthorized changes to (Small Comp’s) IT systems or information.
* Attempt to access data that they are not authorized to use or access.
* Exceed the limits of their authorization or specific business need to interrogate the system or data.
* Connect any non- (Small Comp) authorized device to the (Small Comp) network or IT systems.
* Store (Small Comp) data on any non-authorized (Small Comp) equipment.
* Give or transfer (Small Comp) data or software to any person or organization.

outside (Small Comp) without the authority of (Small Comp).

Supervisors must ensure that individuals are given clear direction on the extent and limits of their authority regarding IT systems and data.

# Internet and email Conditions of Use

Use of (Small Comp) internet and email are intended for business use. Personal use is permitted where such use does not affect the individual’s business performance, is not detrimental to (Small Comp) in any way, not in breach of any term and condition of employment and does not place the individual or (Small Comp) in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

**Individuals must not:**

* Use the internet or email for the purposes of harassment or abuse.
* Use profanity, obscenities, or derogatory remarks in communications.
* Access, download, send or receive any data (including images), which (Small Comp) considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libelous material.
* Use the internet or email to make personal gains or conduct a personal business.
* Use the internet or email to gamble.
* Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
* Place any information on the Internet that relates to (Small Comp), alter any information about it, or express any opinion about (Small Comp), unless they are specifically authorized to do this.
* Send unprotected sensitive or confidential information externally.
* Forward (Small Comp) mail to personal (non-Small Comp) email accounts (for example a personal Yahoo account).
* Make official commitments through the internet or email on behalf of (Small Comp) unless authorized to do so.
* Download copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.
* In any way infringe any copyright, database rights, trademarks, or other intellectual property.
* Download any software from the internet without prior approval of the IT Department.
* Connect (Small Comp) devices to the internet using non-standard connections.

# Clear Desk and Clear Screen Policy

To reduce the risk of unauthorized access or loss of information, (Small Comp) enforces a clear desk and screen policy as follows:

* Personal or confidential business information must be protected using security features provided for example secure print on printers.
* Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
* Care must be taken to not leave confidential material on printers or photocopiers.
* All business-related printed matter must be disposed of using confidential waste bins or shredders.

# Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

* Working away from the office must be in line with (Small Comp) remote working policy.
* Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
* Laptops must be carried as hand luggage when travelling.
* Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
* Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

# Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only (Small Comp) authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

# Software

Employees must use only software that is authorized by (Small Comp) on (Small Comp’s) computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on (Small Comp) computers must be approved and installed by the (Small Comp) IT department.

**Individuals must not:**

• Store personal files such as music, video, photographs, or games on (Small Comp) IT equipment.

# Viruses

The IT department has implemented centralized, automated virus detection and virus software updates within the (Small Comp). All PCs have antivirus software installed to detect and remove any virus automatically.

**Individuals must not:**

* Remove or disable anti-virus software.
* Attempt to remove virus-infected files or clean up an infection, other than using approved (Small Comp) anti-virus software and procedures.

# Cellular (Voice) Equipment Conditions of Use

Use of (Small Comp) voice equipment is intended for business use. Individuals must not use (Small Comp’s) voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual’s own expense using alternative means of communications.

**Individuals must not:**

* Use (Small Comp’s) voice for conducting private business.
* Make hoax or threatening calls to internal or external destinations.
* Accept reverse charge calls from domestic or international operators unless it is for business use.

# Actions upon Termination of Contract

All (Small Comp) equipment and data, for example laptops and mobile devices including tablets, smartphones, USB memory devices and CDs/DVDs, must be returned to (Small Comp) at termination of contract.

All (Small Comp) data or intellectual property developed or gained during the period of employment remains the property of (Small Comp) and must not be retained beyond termination or reused for any other purpose.

# Monitoring and Filtering

All data that is created and stored on (Small Comp) computers is the property of (Small Comp) and there is no official provision for individual data privacy, however wherever possible (Small Comp) will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. (Small Comp) has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

* Computer Misuse Act 1990
* Data Protection Act 1998

**It is your responsibility to report suspected breaches of security policy without delay to your supervisor, the IT department, the information security department, or the IT helpdesk.**

**All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with (Small Comp) disciplinary procedures.**