Information Security policies

1 INFORMATION SECURITY POLICY

Purpose

C. Wood & Son (Luton) Ltd collects, processes, stores and uses information as part of its business processes as a not for profit organisation. Information may be managed through computerised or manual systems. In all cases C. Wood & Son (Luton) Ltd needs to ensure that adequate controls are in place to ensure information is appropriately available, accurate, secure, and complies with legislative requirements. This information security policy provides management direction and support for information security across C. Wood & Son (Luton) Ltd.

The Information Security Policy documentation serves these purposes:

- To set out C. Wood & Son (Luton) Ltd's intentions in managing information security as part of effective governance
- To provide guidance to users, administrators and developers of information systems on appropriate behaviours and controls required in order to maintain the integrity of information.
- To provide a comprehensive approach to information security across C. Wood & Son (Luton) Ltd
- To set out the means by which information policies and are scrutinised, approved, revised, communicated and monitored.

Scope

This Information Security Policy:
- Applies to all directors, staff, members, contractors and third party organisations used by C. Wood & Son (Luton) Ltd.
- Covers all information handled, stored, processed or shared by C. Wood & Son (Luton) Ltd irrespective of whether that information originates with or is owned by C. Wood & Son (Luton) Ltd.
- Applies to all computer and non-computer based information systems owned by C. Wood & Son (Luton) Ltd or used for C. Wood & Son (Luton) Ltd business.

Policy

Responsibility for the Information Security Policy Documentation

The Information Security Policy Documentation set shall be maintained by Director and individual policies may be delegated to C. Wood & Son (Luton) Ltd staff.

Maintaining the Policy Document set

This policy and subsidiary policies shall be reviewed and updated regularly to ensure that all remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Implementing the Information Security Policy

C. Wood & Son (Luton) Ltd will ensure that all individuals who use information systems or handle sensitive information are aware of and understand the relevant policies that apply and the consequences of non-compliance.

Where necessary, C. Wood & Son (Luton) Ltd will implement appropriate physical and logical controls to restrict access to information systems and information to only authorised users.

Full account of the requirements of the Information Security Policy will be taken in planning, designing, implementing and using IT-based information systems.

C. Wood & Son (Luton) Ltd will use lawful means of monitoring the use of information systems and networks for the purposes of preventing, and detecting breaches of the information security policy.

To determine the appropriate levels of security measures applied to information systems, a process of risk assessment shall be carried out for each system to identify the probability and impact of security failures.

Specialist advice on information security shall be made available throughout C. Wood & Son (Luton) Ltd and C. Wood & Son (Luton) Ltd will ensure that it maintains and applies up-to-date knowledge of risks and mitigations within its information management practices.

All users will be required to abide by C. Wood & Son (Luton) Ltd policies before being authorised for access to C. Wood & Son (Luton) Ltd information systems.

C. Wood & Son (Luton) Ltd will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

Responsibilities for implementing the Information Security Policies

An information security working group, made up of key system administrators, managers and representatives from all relevant parts of the organisation, shall devise and coordinate the implementation of information security controls.

The responsibility for ensuring the protection of IT-based information systems and ensuring that specific security processes are carried out shall lie with the Director.

The implementation and effectiveness of the information security policy shall be reviewed periodically by C. Wood & Son (Luton) Ltd's internal audit function as part of its regular audit programme.

Other Related Policies include:

- Acceptable Use Policy
- Data Protection Policy

2 IT ACCEPTABLE USE POLICY

What you may and may not do when you use C. Wood & Son (Luton) Ltd's IT systems, and the consequences of breaking the rules.

Introduction

It is the responsibility of all users of C. Wood & Son (Luton) Ltd's IT systems, to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

Purpose

This Acceptable Use Policy is intended to provide a framework for such use of C. Wood & Son (Luton) Ltd's IT Systems. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

Scope

Staff, visitors and contractors using C. Wood & Son (Luton) Ltd's IT systems are bound by the provisions of its policies in addition to this Acceptable Use Policy. C. Wood & Son (Luton) Ltd seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, assisting with tasks etc. to the highest possible standards.

Policy

Unacceptable Use

a) The C. Wood & Son (Luton) Ltd network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited "nuisance" emails;
4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of Venue staff or a third party;
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9. material that brings C. Wood & Son (Luton) Ltd into disrepute.

b) C. Wood & Son (Luton) Ltd's network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

1. intentionally wasting staff effort or other C. Wood & Son (Luton) Ltd resources;
2. corrupting, altering or destroying another User's data without their consent;
3. Gaining access to member data for any use other than that of the requirements of C. Wood & Son (Luton) Ltd business.
4. disrupting the work of other Users or the correct functioning of the C. Wood & Son (Luton) Ltd Network; or
5. denying access to the C. Wood & Son (Luton) Ltd Network and its services to other users.

c) Where the C. Wood & Son (Luton) Ltd Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the C. Wood & Son (Luton) Ltd Network.

d) Users shall not:

1. introduce data-interception, password-detecting or similar software or devices to the C. Wood & Son (Luton) Ltd Network;
2. seek to gain unauthorised access to restricted areas of C. Wood & Son (Luton) Ltd's Network;
3. access or try to access data where the user knows or ought to know that they should have no access;
4. carry out any hacking activities; or
5. intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a User C. Wood & Son (Luton) Ltd may in its sole discretion:

a) restrict or terminate a User's right to use the C. Wood & Son (Luton) Ltd Network;
b) withdraw or remove any material uploaded by that User in contravention of this Policy; or
c) where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

In addition, where the User is also a member of the University community, the University may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Charter, Statute, Ordinances and Regulations.

Definitions
C. Wood & Son (Luton) Ltd Network – all computing, telecommunication, and networking facilities provided by C. Wood & Son (Luton) Ltd, with particular reference to all computing devices connected to systems and services supplied.

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

3 ANTI-VIRUS POLICY

Purpose

To establish the requirements for effective virus detection and prevention

Scope

This policy applies to:

- All C. Wood & Son (Luton) Ltd owned or operated computer equipment connected to the C. Wood & Son (Luton) Ltd Network
- All Third-Party computer equipment connected to the C. Wood & Son (Luton) Ltd Network
- All users or administrators of the above computer equipment.

Policy

Use of Anti-Virus software
All computer equipment identified by the scope of the policy shall have anti-virus software installed and operational.

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.

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.

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 Director.

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 C. Wood & Son (Luton) Ltd Computing Facilities.

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.

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 the Director in implementing this policy.

The Director shall be responsible for ensuring that anti-virus software is installed and operating on servers or shared computer equipment.

Related policies, standards and guidelines

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

Enforcement

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

4 EMAIL POLICY

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

Scope
This policy applies to all users who send or receive email via the C. Wood & Son (Luton) Ltd network or from C. Wood & Son (Luton) Ltd email systems, whether accessed from on or off-site.

Policy

Information Services responsibilities
All @cwoodandson.co.uk email entering or leaving the C. Wood & Son (Luton) Ltd network shall pass through the email filtering service and mail relays operated by its email provider.

Email travelling entirely within the C. Wood & Son (Luton) Ltd 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 should 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.

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 C. Wood & Son (Luton) Ltd 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.

Users conducting C. Wood & Son (Luton) Ltd business or communications via email must use a C. Wood & Son (Luton) Ltd provided email account.

Personal email accounts must not be used for conducting C. Wood & Son (Luton) Ltd 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.

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.

Terms and definitions

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.

Enforcement

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

5 PERSONNEL POLICY FOR INFORMATION SECURITY

Purpose

This policy deals with the recruitment, management and departure of staff. It aligns with Human Resources policies. The term Staff in the policies below should be taken to include employees, temporary staff, directors, contractors, consultants, external auditors, volunteers, work placements and partner organisations, wherever there is a contract between them and the C. Wood & Son (Luton) Ltd which requires or allows that party or that party's employees to access C. Wood & Son (Luton) Ltd's information systems or data.

These policies reflect:

- the employment of staff
- and training of all staff
- departing staff
- the special cases of disaffected staff.

Policy on Employing Staff

The Terms and Conditions of Employment and for external parties the Contractual Terms of C. Wood & Son (Luton) Ltd must include the employer's and employee's requirements to comply with information security policies.

Controls and Processes

As part of the Terms and Conditions of Employment, and for external parties the Contractual Terms, all staff are required to sign a formal undertaking concerning the need to protect the confidentiality of information and to follow C. Wood & Son (Luton) Ltd's information security policies, both during and after their employment with C. Wood & Son (Luton) Ltd.

An appropriate summary of the information security policies must be formally delivered to and accepted by any temporary staff, contractor, consultant, external supplier or partner organisation, prior to the supply or use of services.

Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.

All staff are to be provided with information security awareness tools to enhance awareness and educate them regarding the range of threats, the appropriate safeguards and the need for reporting suspected problems.

Enforcement

Any information security incidents resulting from non-compliance should result in appropriate disciplinary action.

Policy on Training

C. Wood & Son (Luton) Ltd is committed to providing training to all users of new system to ensure that their use is both efficient and does not compromise information security.

Controls and Processes

Periodic training for the Director is to be prioritised to educate and train in the latest threats and information security techniques.

All new staff are to receive mandatory information security awareness training as part of induction.

Where staff change jobs or roles, their information security needs must be reassessed and any new training needed should be provided as a priority.

Training in information security and threats and safeguards is mandatory for staff with IT responsibilities, with the extent of training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards.

Policy on Departing Staff

On termination of employment the access privileges of departing staff for C. Wood & Son (Luton) Ltd information assets and systems will be revoked.

Controls and Processes

Departing staff must return all information assets and equipment belonging to C. Wood & Son (Luton) Ltd, unless agreed otherwise with the designated Information Owner responsible for that information asset.

Access privileges will normally be removed on the last contractual day. No further access will be allowed unless another relationship is established between C. Wood & Son (Luton) Ltd and the departing member of staff. Such arrangements must be sanctioned by the Director.

Emails and file spaces of departing staff will be retained and archived.
C. Wood & Son (Luton) Ltd maintains the right to reallocate access to the file store, workspaces and email of departing staff.

Policy on Disaffected Staff

Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with senior management and the Director.

Controls and Processes

Upon notification of staff resignations, dismissal or suspension, senior management must consider with the Director whether the member of staff's continued access rights constitutes an unacceptable risk to C. Wood & Son (Luton) Ltd and, if so, revoke all access rights.
Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges.

6 AUDIT POLICY

Purpose

To provide the authority for staff with IT responsibilities to conduct security audits on IT equipment in order to investigate security breaches or ensure compliance with C. Wood & Son (Luton) Ltd policy or other legal or contractual requirements.

Scope

This policy applies to:

- All C. Wood & Son (Luton) Ltd owned or operated IT equipment.
- All third party IT equipment permanently or temporarily connected to the C. Wood & Son (Luton) Ltd network.
- All users or administrators of the above IT equipment.

Policy

Audits may be conducted to:

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

The Director may carry out an audit on any IT equipment within the scope of the policy. Audits must be conducted by authorised IT staff. PCS-Systems (C. Wood & Son (Luton) Ltd IT Contractors) may also be requested to assist in some circumstances.

Auditors may request and shall expect assistance from users responsible for the IT equipment being audited.

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.

Types of audit Security breach

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 shall facilitate access to the system for the auditor and provide administration level access if requested.
Information collected by authorised network monitoring activities may also be used in conjunction with information collected during the audit to draw conclusions.

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.

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.

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.

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 Director or a designated representative must be informed and the Police notified.

Related policies, standards and guidelines

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

Enforcement

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

7 INFORMATION HANDLING POLICY

Purpose

This policy sets out the need to define classes of information handled by C. Wood & Son (Luton) Ltd and the requirements on the labelling, storage, transmission, processing and disposal of each. Requirements include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups). System documentation should itself be classified as sensitive information. This policy should be familiar to all staff dealing with information.

In addition to needing to meet legal compliance requirements, it is beneficial to C. Wood & Son (Luton) Ltd to achieve and maintain good standards of information handling. This policy identifies the sub-policies, controls and processes required to catalogue, maintain and protect information held and used by C. Wood & Son (Luton) Ltd. C. Wood & Son (Luton) Ltd endorses a culture of proactive risk management relating to information handling, to help reduce risks including: loss of data, unauthorised access, wasted resources, complaints and damage to reputation.

This policy and its sub-policies provide for:

- Inventory and classification of information assets
- Backup, use of removable media and information disposal

Scope

This policy applies to all information assets and data collected, held, used and distributed by C. Wood & Son (Luton) Ltd, in databases, data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information.

This policy and the controls and processes contained within it applies to all of C. Wood & Son (Luton) Ltd's employees and any of its partners who collect data on behalf of the C. Wood & Son (Luton) Ltd or receive data provided by C. Wood & Son (Luton) Ltd.

Policy

C. Wood & Son (Luton) Ltd will collect, classify, store, process and distribute its information assets in accordance with the principles of confidentiality, integrity and availability, with custodianship and maintenance of [especially] confidential or highly sensitive, sensitive and personal information being documented and controlled. Sensitive (or high classification of) information should only be stored, transferred or copied when the confidentiality and integrity of the data can be reasonably assured throughout the process, including those processes that involve partner organisations.

7.1 INVENTORY AND CLASSIFICATION OF INFORMATION ASSETS POLICY

Policy statements

All information used for, or by C. Wood & Son (Luton) Ltd, must be filed appropriately and according to its classification. An inventory will be maintained of all C. Wood & Son (Luton) Ltd's major information assets and the custodian of each asset will be clearly stated. Within the information inventory, each information asset will be classified according to sensitivity using C. Wood & Son (Luton) Ltd's agreed information security classification scheme. Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium.

Controls and Processes

Information assets should be documented in a form that is easily maintainable e.g. a spreadsheet, containing useful information about each information asset identified including:

- Description or descriptive name.
- Location(s) of the information asset.
- Staff member with responsibility for handling the information or managing the information asset.
- The type(s) of information stored or processed.
- Origin or custodian of the information stored or processed.
- The importance of the information stored or processed.
- Any special or non-standard security measures required

This document should be reviewed regularly by the information custodian, as identified by their position. The C. Wood & Son (Luton) Ltd list of information custodians by job role is set out in the Information Custodians section.

Information assets include, but are not limited to, data in databases and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information

Information assets should be classified according to sensitivity of the data, criteria for which are set out in the Data Classification section:

- Highly sensitive or confidential
- Sensitive
- Personal
- Internal usage
- Public domain or unclassified

Periodically reviewing and updating the list of important information assets is recommended. Performing at least a basic non-technical review of how the information involved is handled may help to identify one of these common problems that can lead to a security incident:

- Expectations differing between the information owner(s) and staff responsible for handling the information. e.g.:
    - The information custodian incorrectly assumes their data is being regularly backed up.
    - The information custodian incorrectly thinks someone else is looking after the security configuration of the system where it is stored.
    - Staff handling documents do not realise they should be locked away out of sight when not in use.
- The handling requirements appropriate for the information in question are unknown therefore suitability of the measures in place is in doubt. e.g.:
    - A file of sensitive personal information is found stored in an insecure area.

Information Custodians

Personal Data	**Information Asset Custodian**
Payroll Records	Finance Manager
HR Records	Director
Website Data	Director
Sage Accounts system	Office Manager
Accident Report Records	Facilities Manager
CCTV Recordings	Director
User Identity & User Server Records	Director
Server Back-ups	Director
Network Security	Director

Non-Personal Data	**Information Asset Custodian**
Finance Records	Finance Manager
Health & Safety Statistics	Facilities Manager
Board Committee agendas & minutes	Director

7.2 BACKUP, USE OF REMOVABLE MEDIA AND INFORMATION DISPOSAL

Policy Statements

All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files.

Day to day data storage must ensure that current information is readily available to authorised users and that archives are both created and accessible in case of need.

Information owners must ensure that appropriate backup and business continuity / system recovery procedures are in place. Backup of C. Wood & Son (Luton) Ltd's information assets and the ability to recover them is an important priority. Information custodians are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of their business.

Information custodians must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace more recent files.

The archiving of information and documents must consider legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with C. Wood & Son (Luton) Ltd's information retention policy.

Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents.

All employees to be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents.

Controls and Processes

All signatures authorising access to systems or release of information must be properly authenticated.

All hard copy documents of a sensitive or confidential nature are to be shredded or similarly destroyed when no longer required. The information custodian must authorise or initiate this destruction.

Any third party used for external disposal of C. Wood & Son (Luton) Ltd's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with C. Wood & Son (Luton) Ltd's information security policies and also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non-compliance.

Highly sensitive or critical documents should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports should normally be self-contained and contain all the necessary information.

Data Classifications

Unclassified / Public domain	Information which is not confidential or personal and which may be disseminated within the organisation and without. An example is the sports information leaflet
Internal	Data which is concerned with the running of C. Wood & Son (Luton) Ltd prior to it becoming public domain. Examples include company year-end accounts.
Personal	Data which enables an individual to be identified; data which relates to or is about an identifiable individual. Such data may be processed lawfully C. Wood & Son (Luton) Ltd provided that staff comply with the DPA and C. Wood & Son (Luton) Ltd's notification.
Confidential / Sensitive	Personal data consisting of information as to— (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs or other beliefs of a similar nature, (d) whether they are a member of a trade union, (e) their physical or mental health or condition, (f) their sexual life, (g) the commission or alleged commission by them of any offence, (h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. Such data may be processed lawfully by C. Wood & Son (Luton) Ltd provided that staff comply with the DPA and C. Wood & Son (Luton) Ltd's notification.

8 USER MANAGEMENT POLICY

Purpose

While it is imperative that users can access the systems and data they require to carry out their business it is necessary to minimise the risks of unauthorised access for both legal and business reasons.

These policies enable information and system owners to establish proper access levels for systems users, and include guidelines in the event of termination of employment.

Policies with controls and processes follow for:

- User password management
- Access control, including eligibility for and review of access rights
- Privilege management

Additional controls and processes are recommended for:

- Staff leaving C. Wood & Son (Luton) Ltd's employment
- Contractors and visitors
- Connection to the internet

8.1 User Password Management

Policy

All users shall have a unique identifier (User ID) for their personal and sole use for access to all computing services. Users will access information systems using this User ID and an associated personalised password.

Controls and processes

The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.

A user may have multiple User IDs to enable them to access separate information systems, each of which shall have separate passwords.

A password is “Confidential authentication information composed of a string of characters” used to access computer systems.

Passwords must be kept confidential. Passwords are the responsibility of individual users; they must not be used by anyone else even for a short period of time. Giving an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence.

Passwords must be at least 6 characters in length. They should be a mix of upper and lowercase, numeric and use other characters such as # @ $ * etc. It is good practice to lock the workstation passwords in multiple occupancy offices, and essential in public areas.

If password confidentiality is compromised in any way, or is found to be weak or non-compliant, the password must be changed immediately.

Password management procedures shall be put into place by the Information System Owner to ensure the implementation of the requirement of the Information Security Policy and to assist users in complying with best practice guidelines.

All information system managers will ensure their systems enable password changes as needed.

No staff should be given access to a live business application system unless trained and made aware of their security responsibilities.

8.2 Access Control to Information Systems

Policy

Procedures for the registration and deregistration of users and for managing access to all information systems shall be established by their information owners to ensure that all user's access rights match their authorisation. These procedures shall be implemented only by suitably trained and authorised staff.

Controls and Processes

Staff and contractors should only access systems for which they are authorised.

Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation.

All contracts of employment, and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information, the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

Access control standards (detailing who is allowed access to which system) must be established for all information systems at an appropriate level for each system, which minimises information security risks yet allows C. Wood & Son (Luton) Ltd's business activities to be carried out without undue hindrance.

Disciplinary Process

Where there is found to have been a deliberate attempt at unauthorised access, or to subvert the controls on access to C. Wood & Son (Luton) Ltd information systems and data, C. Wood & Son (Luton) Ltd may initiate the appropriate disciplinary processes.

8.3 Management of System Privileges

Policy

Access to all systems must be authorised by the information system owner and a record maintained of all authorisations, including the appropriate access rights or privileges.

Controls and Processes

Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organisation.

Users' access rights will be reviewed at regular intervals.

Additional Controls and processes

Staff leaving C. Wood & Son (Luton) Ltd's employment

When a member of staff leaves the employment of C. Wood & Son (Luton) Ltd, their email account record will be ended as part of the termination action.

Prior to an employee leaving, or to a change of duties, line managers should ensure that:

- The employee is informed in writing that he/she continues to be bound by their signed confidentiality agreement, for example during an exit interview.
- Passwords are removed, disabled or changed to deny access.
- Relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists.
- Supervisors passwords allocated to the individual should be removed and consideration given to changing higher level passwords, to which they have access.
- Where appropriate, staff working out notice are assigned to non-sensitive tasks, or are appropriately monitored.
- Departmental and C. Wood & Son (Luton) Ltd property is returned.

Particular attention should be paid to the return of items which may allow future access. These include, keys, manuals and documents.

The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee.

Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment.

Once an employee has left, it can be impossible to enforce security disciplines, even through legal process.

Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

The Director will delete or disable all identification codes and passwords relating to members of staff who leave the employment of C. Wood & Son (Luton) Ltd on their last working day.

Prior to leaving, the employee's manager should ensure that all PC files of continuing interest to the business of C. Wood & Son (Luton) Ltd is transferred to another user before the member of staff leaves.

It is good practice for an 'exit' interview to be held during which the manager notes all the systems to which the member of staff had access and informs the Director of the leaving date.

Managers must ensure that staff leaving C. Wood & Son (Luton) Ltd's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to C. Wood & Son (Luton) Ltd information and equipment.

Contractors and Visitors

All visitors to Departments should have their arrival and departure times recorded. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left.

Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

9 USE OF COMPUTERS POLICY

Purpose

This sets out the responsibilities and required behaviour of users when accessing C. Wood & Son (Luton) Ltd information systems. Policies, controls and processes include those for:

- User identification (see also "User Management Policy")
- Protection against malicious and mobile code
- Back-up
- Exchange of Information
- Operating system access control (see "User Management Policy")

User identification

Policy

All users with their own computer shall have a unique identifier (User ID) for their personal and sole use for access to the C. Wood & Son (Luton) Ltd network and server. (See also "User Management Policy") Users shall be required to follow good security practices in the selection and use of passwords.
In the cases of front of house computers then a 'shared' User ID will be used and password known by the relevant staff only. These computers will have very little confidential information contained on them, with restricted server file access.

Staff will also have other individual passwords to access other systems required to fulfil their role.

Controls and Processes

The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.

Effective password control is important to securing IT systems and data from compromise or misuse. Users are required to comply with rules published by C. Wood & Son (Luton) Ltd for construction, use and management of password.
A robust password policy must be in place for all IT systems. The password policy implemented must include password complexity, periodic change, account lock-out policy.

9.1 Protection Against Malicious and Mobile Code

Policy

Information system owners must ensure that both portable (e.g. laptops) and non-portable (e.g. desktops) equipment is suitable secured - especially when left unattended to avoid risk of interference or misuse.

Files downloaded from the internet that include mobile code and files attached to electronic mail must be treated with the utmost care to safeguard against malicious code and inappropriate material.

Employees are not permitted to load unlicensed software onto C. Wood & Son (Luton) Ltd PCs, laptops or workstations without expressed permission from the Director or PCS Systems (IT Contractors).

Controls and processes

Information system owners must ensure that equipment that will connect to their information systems and could be left unattended has appropriate security protection and that every reasonable precaution has been taken to ensure that unauthorised persons do not gain access to their information systems through unattended equipment.

C. Wood & Son (Luton) Ltd or PCS Systems will disconnect or block, pending investigation, any device or computer on the C. Wood & Son (Luton) Ltd network that is detected as having abnormal traffic activity.
Abnormal traffic patterns, can indicate the presence of a virus or malicious code.

All C. Wood & Son (Luton) Ltd desktop and laptop computers must have an up to date antivirus product. Any non - C. Wood & Son (Luton) Ltd computer being used to access C. Wood & Son (Luton) Ltd systems directly e.g. via VPN, must have an up-to date antivirus product.

A periodic review of executable software held on C. Wood & Son (Luton) Ltd's equipment should be carried out.

9.2 Data Back-up Policy

Policy

C. Wood & Son (Luton) Ltd's main server is backed-up daily, off site.
Any essential information should not be stored on a laptop or on a PC's local disk.

Controls and processes

Server back-ups are encrypted and taken off-site daily. C. Wood & Son (Luton) Ltd's IT contractors (PCS Systems) monitor the success and regularity of back-ups and alert where necessary.

There is also an encrypted back-up conducted daily on a NAS drive connected and stored in the same room as the server. This server is located in a strong room which is kept locked when not in use.

Staff should ensure personal and sensitive data is not stored on high risk media (e.g. usb sticks, portable hard disks).

9.3 Exchange of Information

Policy

Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality is maintained, that it is correctly addressed and that the recipients are authorised to receive it.

Sensitive or confidential data should only be accessed from equipment in secure locations.

Sensitive or confidential data must never be printed on a network printer that does not have adequate protection or security.

Confidential and sensitive information must be secured and encrypted.

Utmost care must be used when transporting files on removable media (e.g. disks, CD-ROMs and USB flash drives, including devices that incorporate such facilities such as mobile phones).

Controls and processes

Before any data or file is imported from removable media the removable media must be scanned.

Confidential and sensitive data must be authorised for removal

Employee e-mail relating to the business of C. Wood & Son (Luton) Ltd is subject to the Freedom of Information Act and the Data Protection Act.

10 MOBILE COMPUTING POLICY

Purpose

As modern mobile computing devices can carry information assets away from C. Wood & Son (Luton) Ltd's premises (and security precautions) those information assets may be subjected to increased risk e.g. loss or theft.

Mobile Computing

Policy

The Persons (employees & contractors) accessing C. Wood & Son (Luton) Ltd information systems remotely to support their business activities must be authorised to do so by the Director.

Controls and Processes

A risk assessment of the information asset being accessed must be carried out by the Director together with the information asset owner especially if the information asset is being accessed using non-C. Wood & Son (Luton) Ltd equipment.

Sensitive or confidential data must not be copied, replicated or downloaded to mobile or remote devices without the permission of the information asset owner.

Where permission is granted, adequate steps must be taken by the user to protect sensitive or confidential data whilst it exists on the mobile or remote device.

C. Wood & Son (Luton) Ltd will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to C. Wood & Son (Luton) Ltd's Information Security policy and other good practices.

Loss of equipment (C. Wood & Son (Luton) Ltd or non-C. Wood & Son (Luton) Ltd) that has been used to access C. Wood & Son (Luton) Ltd's information assets or that may have a copy of some or part of C. Wood & Son (Luton) Ltd's information assets must be reported to the Director.

For the avoidance of doubt, equipment in this case includes any device that can access data or hold data in a retainable form (e.g. hard disks, CD-ROMs and USB flash drives, including devices that incorporate such facilities such as mobile phones)

The loss of sensitive or confidential data held on mobile or remote devices may be treated as a disciplinary issue by C. Wood & Son (Luton) Ltd, especially where there is evidence of carelessness or failure to follow recommended procedures.

11 GUIDE TO INFORMATION SECURITY FOR MOBILE DEVICES

Background

There have been a number of stories in the press and media in recent years about personal and confidential data being lost whilst in transit, laptops left in cafes, child benefit data CDs being lost.

Such losses cause public anxiety around identity theft, undermine the confidence and reputation of organisations involved and can potentially lead to litigation and severe penalties.

The problems of moving data about securely are not new but the technologies available are changing. For example, new mobile devices such as Smart phones have capabilities for information access and mass storage and present risks similar to laptop computers.

The purpose of this information is to give some guidance to staff on recommended practice around using mobile devices to store documents, files or data.

The guidance should be read in conjunction with C. Wood & Son (Luton) Ltd's Information Security Policy and Data Protection Policy.

What are Mobile Devices?

For the purpose of this guidance, mobile devices are classified as any device holding data which is likely to be carried from place to place and includes:

- Laptop computers, tablets
- USB Stick/Pen drives
- Mobile phones (especially smart phones)
- CD/DVD ROMs
- Portable hard drives

These portable devices are more prone to being lost due to the nature of their portability.

Laptops, phones and hard drives are highly desirable and therefore attractive to thieves.

You must assume that in the case of loss or theft, the data stored on these devices is potentially then accessible to unauthorised people.

For this reason it is essential that you are aware of the risks and take extra precautions.

Your Responsibility

Anyone who stores, or transports data and information concerned with the operation of C. Wood & Son (Luton) Ltd, using mobile devices, is deemed by C. Wood & Son (Luton) Ltd to be responsible for the security of that data in transit and must take adequate and appropriate steps to safeguard it.

If there is a loss or unauthorised disclosure of confidential, sensitive or personal data from C. Wood & Son (Luton) Ltd due to poor practice or negligence on your part, disciplinary action may be taken against you, where the ultimate sanction is dismissal from C. Wood & Son (Luton) Ltd.

Required Practices with Mobile Devices

All users are required to abide by the following practices:

1. You must not store confidential/sensitive or personal data e.g. info relating to living individuals that has been provided by C. Wood & Son (Luton) Ltd, on a mobile device without prior authorisation from the data owner or custodian. You may not save copies or extracts of staff records, without expressed permission.

    a. confidential/sensitive or personal data stored on a mobile device, must be encrypted using a minimum of AES 128 bit encryption with a strong key/password of at least 10 characters (see password guidelines).

2. Any device that pulls e-mail from C. Wood & Son (Luton) Ltd systems e.g. Smartphone, android, iPhone etc, whether owned by C. Wood & Son (Luton) Ltd or by the individual, must be effectively protected with a system authenticated password.

3. Sensitive or confidential data should, ideally, not be passed by e-mail. Where this unavoidable, it must be encrypted.

4. Disable Wi-fi and Bluetooth when you don't need them. Not only does this make your mobile device more secure but saves on the battery use. Disabling/enabling these features varies from device to device - your lap-top and Smartphone manuals will contain the details.

5. Avoid accessing or transmitting sensitive/confidential data when connected to public and open wi-fi hot spots.

6. When using your laptop in public spaces e.g. on trains, airport lounges, you must take care over what can be seen on your screen.

7. Care should be taken to protect mobile devices from theft:

- Lock laptops, and tablet computers in the boot when parked or travelling by car
- Don't leave your laptop or phone in an unattended car - 50% of thefts are from vehicles
- Take extra care and be vigilant in public spaces and on public transport
- Make sure you lock the office door when leaving equipment unattended

8. All lost or stolen devices that contain confidential, sensitive or personal data belonging to C. Wood & Son (Luton) Ltd must be reported immediately to the Director and where appropriate (laptop, phone) to the police.

9. Mobile phone apps represent a new risk from malware and viruses. Downloaded apps can incorporate undesirable code which open your phone up for hacking. Only buy from dedicated app stores and avoid downloading pirated apps. Be cautious and wary of software downloads and their origins.

10. E-mail concerning C. Wood & Son (Luton) Ltd business is discoverable under freedom of information and data protection legislation. Therefore you must take care when writing e-mails, not to be liable or be derogatory about individuals or organisations. Always assume that those mentioned in an email are free to read the e-mail if they so wish.

11.1 Classification of data for security purposes

1.	Confidential/Highly sensitive	Data which may or may not be personal and which should not be disclosed except where authorised e.g. disciplinary proceedings or investigations
2.	Sensitive	Personal data consisting of information relating to religious belief, political opinions, sexuality, physical or mental health, court action etc
3.	Personal	Data which enables individuals to be identified or relates to an identifiable individual. This can be processed lawfully by C. Wood & Son (Luton) Ltd provided that staff comply with the DPA and C. Wood & Son (Luton) Ltd's notification
4.	Internal	Data which is concerned with the running of C. Wood & Son (Luton) Ltd prior to it becoming public domain e.g. committee papers
5.	Unclassified /Public domain	Information which is not confidential or personal and which may be disseminated within C. Wood & Son (Luton) Ltd and without.

12 ENCRYPTION POLICY

Purpose
To define the minimum requirements for the safe encryption of data

Scope
This policy applies to all users of C. Wood & Son (Luton) Ltd equipment.

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.

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.

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.

13 Network Monitoring Policy

Purpose

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

Scope

This policy applies to:

- All IT equipment locally connected to the C. Wood & Son (Luton) Ltd network.
- All IT equipment remotely connected to the C. Wood & Son (Luton) Ltd network whilst the equipment is connected to the C. Wood & Son (Luton) Ltd 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.

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 C. Wood & Son (Luton) Ltd communications systems.

The primary aims of network monitoring are:

- To maintain the integrity and security of the C. Wood & Son (Luton) Ltd network, IT equipment and information assets.
- To collect information to be used in network design, engineering, troubleshooting and usage-based accounting.

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).

Enforcement

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

14 Network Access Control

Purpose

To establish the requirements for connection of IT equipment to the C. Wood & Son (Luton) Ltd network.

Scope

This policy covers all IT equipment locally connected to the C. Wood & Son (Luton) Ltd network. Computer equipment remotely connected to the C. Wood & Son (Luton) Ltd network is covered by the Remote Access and Virtual Private Networking Policy.

Policy

C. Wood & Son (Luton) Ltd Network

The C. Wood & Son (Luton) Ltd network consists of a wired network accessed via plug-in data points in C. Wood & Son (Luton) Ltd building and a wireless network accessed via broadcasts from wireless access points around the venue.

C. Wood & Son (Luton) Ltd's network is operated by Director and IT Contractors (PCS).

Computer equipment is attached to the wired network by connection to a plug-in data point using a compatible network cable.

C. Wood & Son (Luton) Ltd operates a managed switch which separates various uses required by the business.

Ports are separated as follows for security and operation purposes:

- Staff main network
- PDQ usage
- Staff main network WIFI access points (SSID C. Wood & Son (Luton) Ltd Int)

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).

All C. Wood & Son (Luton) Ltd-owned IT equipment to be connected to the wired network must be registered with Heads of Departments prior to connection.

Users must not change the hardware address associated with an item of computer equipment connected to the wired network.

Personal network equipment, including wireless access points, shall not be connected to the C. Wood & Son (Luton) Ltd network.

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 C. Wood & Son (Luton) Ltd network unless the wireless access point or network routing features are disabled.

15 Remote Access and Virtual Private Network Policy

Purpose

To establish the requirements for safe use of remote connections to the C. Wood & Son (Luton) Ltd network off-site.

Scope

This policy applies to:

- Remote access policy requirements apply to all users remotely connecting to the C. Wood & Son (Luton) Ltd network off-site.
- All users employing VPN technology to remotely connect to the C. Wood & Son (Luton) Ltd network from off-site locations via the Information Services supported VPN gateway.
- All users requiring a VPN connection from the C. Wood & Son (Luton) Ltd network, through the firewall, to a VPN terminator outside the C. Wood & Son (Luton) Ltd network and operated by a third party.

Policy

General Remote access users should note that by connecting to the C. Wood & Son (Luton) Ltd network they become part of the C. Wood & Son (Luton) Ltd network and must treat any computer connected in this way as if it were on the C. Wood & Son (Luton) Ltd premises.

In particular they must follow the requirements and recommendations of the Code of Practice for Users of the C. Wood & Son (Luton) Ltd 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.

Service requirements Remote access allows users to connect to the C. Wood & Son (Luton) Ltd 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.

C. Wood & Son (Luton) Ltd plays no part in provision of the service. Remote access to the C. Wood & Son (Luton) Ltd 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 C. Wood & Son (Luton) Ltd 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 C. Wood & Son (Luton) Ltd network is provided to allow C. Wood & Son (Luton) Ltd members to perform legitimate business 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 site location.

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.

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 C. Wood & Son (Luton) Ltd Computing Facilities, the Mobile Computing Policy, the Personal Computer Security Policy, the AntiVirus Policy, the Password Policy and the Email Policy.

Enforcement

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

16 OUTSOURCING AND THIRD PARTY ACCESS

Purpose

C. Wood & Son (Luton) Ltd uses third parties (e.g. contractors, suppliers and outsourcing) to help create and maintain its information assets.

It also allows connectivity to some of those information assets to external organisations (e.g. customers). This access needs to be controlled.

This policy area is designed to ensure that external parties that attach to and utilise information in C. Wood & Son (Luton) Ltd's information systems are aware of and comply with C. Wood & Son (Luton) Ltd's Information Security policies policy.

Policy on Information Security around outsourcing and third party access

All third parties who are given access to C. Wood & Son (Luton) Ltd's information systems, whether as suppliers, customers or otherwise, must agree to follow C. Wood & Son (Luton) Ltd's Information Security policies.

Confidentiality agreements must be used in all situations where the confidentiality, sensitivity or value of the information being accessed is classified as personal, sensitive or confidential/highly sensitive (see Information Handling Policy for explanation of classifications].

All contracts with external suppliers for the supply of services to C. Wood & Son (Luton) Ltd must be monitored and reviewed to ensure that information security requirements are being satisfied.

Controls and Processes

An appropriate summary of the information security policies and the third party's role in ensuring compliance must be formally delivered to any third party prior to their being granted access.

Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the contents and spirit of C. Wood & Son (Luton) Ltd's Information Security policies.

Persons responsible for commissioning outsourced development of computer based systems and services must use reputable companies that operate in accordance with recognised quality standards and which will follow the information security policies of C. Wood & Son (Luton) Ltd, in particular those relating to application development.

Any facilities management, outsourcing or similar company with which C. Wood & Son (Luton) Ltd may do business must be able to demonstrate compliance with C. Wood & Son (Luton) Ltd's information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

Management of access for partner organisations and external staff

Depending on the partnership arrangements, staff of partner organisations who are assisting C. Wood & Son (Luton) Ltd or delivering programmes of study may need access to C. Wood & Son (Luton) Ltd information systems.

All external users who need to access the C. Wood & Son (Luton) Ltd's systems or secured information assets must speak with a senior member of staff.

The senior member of C. Wood & Son (Luton) Ltd staff who is responsible for maintaining the operational relationship between the C. Wood & Son (Luton) Ltd and the third party must confirm the appropriateness of access requests, and advise the Director of changes in relationships e.g. need to withdraw user access.

External users who require access to C. Wood & Son (Luton) Ltd information systems must formally acknowledge and agree to comply with the C. Wood & Son (Luton) Ltd Information Security policy and procedures and completed the appropriate External Access Request Form.

In accepting the terms of access, the partner undertakes to take all necessary steps to protect C. Wood & Son (Luton) Ltd's information assets from unauthorised access, misuse or disclosure. This includes ensuring appropriate controls are in place on local workstations including: up to date anti-virus, anti-spyware and security patches; not sharing ID and passwords; logging out when systems are not being used.

All external access arrangements will be reviewed at least annually to confirm that 3rd party users continue to have appropriate levels of access for their role.