Information Security Policy

Version: 0.2
Date:20.03.2023
Created by: GDPR Local
Stored at: Safe storage

Introduction

We all hold personal data about our employees, clients, suppliers, and other individuals for a variety of purposes. The information security system within our company is aimed at protecting employees, partners, clients, data subjects, and customers of the company from illegal or damaging actions by individuals, either directly or implied, knowingly, or unknowingly, when processing information and data which come at their disposal, as well as using certain equipment for the fulfilment of their work duties.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access to in the course of their work.

The policy shall apply to the processing of information within any systems or held on any media involved in the data/information processing within the company, irrespective of whether data/information processing is related to internal operations of the company or to external relations of the company with any third parties.

Scope

This policy applies to all staff, systems, data subjects, and third parties. We may supplement or amend this policy with additional policies and guidelines from time to time. Our Data Protection Lead has overall responsibility for the day-to-day implementation of this policy.

More details can be found in the following documents:

Data Retention and Erasure Policy
Information Classification Policy

Information Security Policy Statement

It is our policy to use all reasonably practicable measures to ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information is assured

- Integrity of information is maintained
- Regulatory and legislative requirements will be met
- Business Continuity plans has been produced, maintained and tested
- The Conservatory Insulation Company requirements for availability of information and information systems will be met
- The rights of all data subjects are protected at all times
- We are able to respond to requests from data subjects professionally and courteously

All breaches of information security, actual or suspected, must be reported to the appropriate person. Breaches of the security policies will be investigated in accordance with the company's operational procedures.

Cyber Essentials

Our policy is based on implementation and ongoing management of comprehensive cyber security capabilities. For example:

Firewall

- We will ensure an appropriate firewall is in place to protect our internet connection

Devices

- We will ensure the highest level of security setting on all devices
- We will remove devices and services we do not use from the network
- We will use appropriate user access / password controls

Access Control

- We will establish appropriate access control processes and mechanisms
- We will only use licensed software and devices

Virus and Malware Protection

We will install appropriate virus and malware protection mechanisms

Updates

We will ensure software and devices are updated regularly. The following

sections define these requirements in more detail.

Definitions

Purposes Of Personal Data

The purposes for which personal data may be used by us includes, but is not limited to:

- Personnel
- Administrative
- Financial
- Regulatory
- Payroll and business development purposes
- Business operation
- Developing and growing our business
- Providing our services to our clients
- Protecting our business interests
- Recruitment and selection services

Business purposes

Business purposes include the following

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons - providing our services to our clients
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct
- Marketing our business
- Improving services
- Growing and developing our business and the services we provide

- Realising the value of the company by disposing of assets including data
- Recruitment and selection services

Personal Data

Information relating to identifiable individuals, such as

- Consultants [prospective, current, ex]
- Candidates / job applicants
- Current and former employees
- Agency staff
- Contractors and other staff
- Clients [customers, partners, etc…]
- Suppliers, partners, sub-processors, and other third parties
- Marketing contacts
- Details of data subjects / individuals collected during our investigations and as required to provide our services
- All other data subjects

Sensitive Personal Data

We do not routinely collect sensitive personal data, but if we do, we will ensure that we implement all the necessary and appropriate safeguards to protect such data.

Fair processing

We must process personal data fairly and lawfully in accordance with individuals' rights. In some cases, this means that we should not process personal data unless the individual whose details we are processing has consented to this happening or where we are confident that the balance of legitimate interest is a reasonable lawful basis on which to operate.

We may process personal data without explicit consent, in these cases we will ensure we have an alternative lawful basis under which to operate. For example, where we, or our clients have a legitimate interest or legal obligation to process the data.

Where we use Legitimate Interest as our lawful basis, we will complete a Legitimate Interest assessment and where necessary a DPIA to ensure we take appropriate care of all data. For example, as defined in Article 9.2.f. of the GDPR.

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law and to comply with legal obligations, for example Health and Safety at Work regulations. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Roles and Responsibilities

Company responsibilities

- Staying updated on data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff
- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the other team members to ensure all marketing initiatives adhere to data protection law and the company’s data protection policy
- Researching third-party services (such as cloud services) that the company is considering using to store or process data members and those included in this policy

- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by The Conservatory Insulation Company
- Checking and approving with third parties that handle the company's data, any contracts or agreement regarding data processing
- Ensuring all staff, contractors, and other third parties are trained to a level appropriate to their role and data access privileges. Records of training must be maintained as part of our compliance and audit procedures.

Data Security – Personal Responsibilities

It is the responsibility of everyone to keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, it will be established what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

All staff, contractors, consultants should receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided whenever there is a substantial change in the law or to our policy and procedure. Completion of training is compulsory.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact your manager or other appropriate person.

Security Policies

Summary of Main Security Policies

The following to be applied as appropriate to our organisation:

- Confidentiality of all company data is to be maintained through discretionary and mandatory access controls
- Access is restricted to authorised personnel only

- Access to data on all laptop computers is to be secured through encryption or other means to provide confidentiality of company data in the event of loss or theft of company equipment
- Only authorised software may be installed
- The use of unauthorised software is prohibited. In the event of unauthorised software being discovered it will be removed immediately
- Data may only be transferred for approved purposes.
- All removable media from external sources [e.g. USB drives] must not be attached to our computer equipment unless prior approval is granted
- All removable media from external sources [e.g. USB drives] must be virus scanned prior to any file, media, content being accessed
- All removable media must be securely disposed of after each use - removable media should not be reused
- Passwords must conform to company requirements
- The physical security of computer equipment will conform to company requirements
- To prevent the loss of availability of company IT resources measures must be taken to backup data, applications and the configurations of all devices

Virus Protection

- Care should be taken when using external drives or other types of media brought in from outside the company. Possible change with new guidance from Microsoft is that all USB flash drives should be disabled. It's enabled at the moment, but the recommendation is to block this
- Management strongly endorses the company's anti-virus policies and will make the necessary resources available to implement them
- Users will be kept informed of current procedures and policies
- Where necessary, users will be notified of virus incidents
- Employees will be accountable for any breaches of the company's antivirus policies
- Antivirus policies and procedures will be reviewed regularly
- In the event of a possible virus infection the user must inform management immediately. Arrangements will be made to scan the infected machine and any servers or other workstations to which the virus may have spread and eradicate it

Access Control

- Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times
- Where possible no one person will have full rights to any system
- Access to the cloud network/servers and systems will be by individual username and password
- Usernames and passwords must not be shared by users
- Usernames and passwords should not be written down
- Intrusion detection will be implemented where considered necessary and where financially viable
- Users will be given a username and password to login to systems, servers, applications as appropriate
- We will be notified of all employees leaving the company's employment. We will then remove the employees' rights to all systems
- Network/server supervisor passwords and system supervisor passwords will be stored in case of an emergency
- Use of the admin usernames on systems are to be kept to a minimum
- Default passwords on systems and other resources will be changed after installation

Network Security

Hubs/Switches

- LAN (Local area network) equipment, hubs, bridges, repeaters, will be secure

Workstations

- Users must log out of their devices when they leave their devices for any length of time
- All unused devices must be switched off outside working hours

Wiring

- All network wiring will be documented

Servers

- All servers will be made securely with all appropriate measures taken to ensure data is protected, backed-up, and safe at all times

Inventory Management

- IT will keep a full inventory of all computer equipment and software in use throughout the company
- Computer hardware and software audits will be carried out periodically. These audits will be used to track unauthorised copies of software and unauthorised changes to hardware and software configurations

Internet Security

- Permanent connections to the Internet will be via the means of a firewall to regulate network traffic
- Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic
- Automation of security policies are deployed down to all devices and user profiles to protect and govern systems in use

Email Security

- If an email is received from an unknown source and you are unsure of its legitimacy, then delete it and please inform the appropriate person
- When you start to type in the name of the recipient, email software will suggest similar addresses you have used before. If you have previously emailed several people, whose name or address starts the same way - e.g. “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone
- When forwarding emails ensure that company privacy is protected at all times, especially when forwarding a chain of emails
- Email should always be constructed in a professional manner as the

email you are sending is representing the company and the brand the recipient could forward that email onto another party

- When sending company data, you must avoid doing so in an anti-competitive way. This includes but is not limited to, price fixing, restricting competitors selling your product, bid rigging, failure to abide by this rule will be dealt with through the disciplinary system

Data Storage

- All data and information collected and processed in any form (paper, electronic etc.) shall be subject to the requirements of this policy. Any regulation in respect to collection, processing, protection and retention of data/information and such documents shall be stored in a safe place as designated by the company for a retention period provided for by applicable laws and/or indicated by the company
- Employees are not permitted to keep any confidential information on mobile devices [phone, laptop, tablet] except information which is temporarily needed for specific, work related activity. Any download of such files to local devices should be avoided or limited only to necessity related with information processing for work purposes
- Internet access and operations performed by employees according to the requirements of the applicable laws and regulations may be filtered and monitored by duly authorised personnel of or on behalf of the company
- Any mobile, portable devices (including laptops, tablets, smartphones and other handheld computing devices) as well as any cloud information storage places should be approved by the company and secured to prevent unauthorised access
- Only systems and program software licensed and authorised by the company can be installed and used on equipment and tools used within the company. Before downloading or installing any software to devices held and used by employees for the purposes described in this policy permission from the management team shall be obtained
- In cases when employees use home devices the employees shall be obliged to comply with the requirements of this policy; equally as if they were using equipment provided by the company. Accordingly, it shall be prohibited to store any data and information related to the company on the device; any processing of the data shall be permitted only through cloud and online storage places used by the company
- In case access is granted to the employee to a system of a client or cooperation partner of the company; the employee shall be obliged to use the access tools provided by the client or partner and follow

provided guidelines on secure information/data processing requirements (including use of encryption systems, passwords, data use limitations, using dedicated locations etc.)

- No information/data referred to in this policy shall be sent, forwarded, or otherwise submitted to any third party, unless it is necessary for the accomplishment of work duties of the employee. In the case of forwarding and submission of data to third parties, it shall be ensured that the data is protected and corresponding security measures have been taken
- The company shall audit the systems used in the processing of information/data to control ongoing compliance with this policy and applicable statutory requirements

Data Retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons why that personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. For more information refer to the Data Retention and Erasure policy document.

Encryption And Anonymisation Policy

Encryption protects information stored on mobile and static devices and in transmission. It is a way of safeguarding against unauthorised or unlawful processing of data. There are a number of different encryption options available.

Anonymisation of personal data should be considered where possible and desirable. Anonymisation ensures the availability of rich data resources, whilst protecting individuals' personal data.

The company will consider encryption alongside other technical measures, taking into account the benefits and risks that it can offer. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere without first consulting the appropriate

person.

Prohibited Activities

Save for exceptions specifically established; in no case and under no circumstances should any equipment, systems or tools owned by the company, its clients or cooperation partners be used for purposes not related to work duties of the employee or not related to business operation of the company.

The Following Activities Are Prohibited, With No Exceptions

Breach of this policy can lead to disciplinary action and other legal action.

- Installation, copying, distribution or storage on any The Conservatory Insulation Company systems or equipment of any illegal software, online platforms, any other electronic contents which are not licensed for use of by The Conservatory Insulation Company
- Violation of the rights of any person by excessive and unnecessary collection and processing of personal data
- Accessing data, server or an account for a purpose other than conducting business operation of The Conservatory Insulation Company or performance of work duties of the particular employee
- Exporting of software, technical information, encryption keys or technology in breach of applicable international or national laws and regulations and/or directions of The Conservatory Insulation Company
- Exporting of any data or information which is of proprietary and/or confidential value to the company, if such exporting is not required in the course of business operation of The Conservatory Insulation Company or performance of work duties of the employee and/or is in breach of internal regulations of the company, applicable laws or regulations
- Revealing an employee’s account password to others and allowing the use of such account by others (including but not limited to employee’s family members)
- Effecting security breaches or disruptions of network communication. Such security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account which the employee is

not expressly authorised to access, unless such access rights are granted to the employee due to him/her being involved in a specific project of the company.

Reporting Security Incidents

- All information/data processing security incidents or threatened incidents shall be immediately reported to management, which accordingly shall take all measures for prevention of potential damage, elimination of the damage caused and restitution of previous security status
- If applicable, it shall be the obligation of the management to ensure further reporting on data/information security breach to all relevant authorities and individuals involved as provided for by applicable laws and regulations and/or laws of England and Wales.

Review

This document should be reviewed annually and amended regularly to ensure compliance.

End.