Data Protection Policy



1. Overview

<FULL COMPANY NAME> (hereafter "<SHORT COMPANY NAME>") establishes this Data Protection Policy, for managing how personal data must be collected, handled and stored to meet the company's data protection standards, and to comply with the law.. The Data Protection Policy program helps <SHORT COMPANY NAME> implement security best practices with regard to meeting the company's data protection standards, and to comply with the law.

2. Purpose

<SHORT COMPANY NAME> security policies serve to be consistent with best practices associated with organizational security management. It is the intention of this policy to establish a data protection capability throughout <SHORT COMPANY NAME> and its business units to help the organization implement security best practices with regard to how all personal data must be collected, handled and stored to meet the company's data protection standards, and to comply with the law. This data protection policy ensures <SHORT COMPANY NAME>:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

3. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <SHORT COMPANY NAME>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <SHORT COMPANY NAME> IT resources (including email, messages and files) is the property of <SHORT COMPANY NAME>. All users (<SHORT COMPANY NAME> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

The Data Protection Act 1998 describes how organizations – including <SHORT COMPANY NAME> – must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

- The Data Protection Act is underpinned by eight important principles. These say that personal data must:
    - Be processed fairly and lawfully

    - Be obtained only for specific, lawful purposes
    - Be adequate, relevant and not excessive
    - Be accurate and kept up to date
    - Not be held for any longer than necessary
    - Processed in accordance with the rights of data subjects
    - Be protected in appropriate ways
    - Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection (only applicable in the EU based companies)
- This policy applies to:
    - The head office of <SHORT COMPANY NAME>
    - All branches of <SHORT COMPANY NAME>
    - All staff and volunteers of <SHORT COMPANY NAME>
    - All contractors, suppliers and other people working on behalf of <SHORT COMPANY NAME>
- It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:
    - Names of individuals
    - Postal addresses
    - Email addresses
    - Telephone numbers
    - …plus any other information relating to individuals
- Data protection risks
    - This policy helps to protect <SHORT COMPANY NAME> from some very real data security risks, including:
        - Breaches of confidentiality. For instance, information being given out inappropriately.
        - Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
        - Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.
    - Responsibilities
        - Everyone who works for or with <SHORT COMPANY NAME> has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:
            - The management team is ultimately responsible for ensuring that <SHORT COMPANY NAME> meets its legal obligations.
            - The Data Protection Officer, is responsible for:
                - Keeping management updated about data protection responsibilities, risks and issues.
                - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
                - Arranging data protection training and advice for the personnel covered by this policy.
                - Handling data protection questions from employees and anyone else covered by this policy.
                - Dealing with requests from individual’s to see the data <SHORT COMPANY NAME> holds about them (also called ‘subject access requests’).

        - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - The IT manager, is responsible for:
        - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
        - Performing regular checks and scans to ensure security hardware and software is functioning properly.
        - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - The Marketing Manager, is responsible for:
        - Approving any data protection statements attached to communications such as emails and letters.
        - Addressing any data protection queries from journalists or media outlets like newspapers.
        - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

4. Policy

<SHORT COMPANY NAME> has chosen to adopt the Data Protection Policy principles established in <STANDARD REFERENCES> as the official policy for this domain. The following subsections outline the Data Protection Policy standards that constitute <SHORT COMPANY NAME> policy. Each <SHORT COMPANY NAME> business system is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- General staff guidelines
    - The only people able to access data covered by this policy should be those who need it for their work.
    - Data should not be shared informally. When access to confidential information is required, employees can request it from their managers.
    - <SHORT COMPANY NAME> will provide training to all employees to help them understand their responsibilities when handling data.
    - Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
    - In particular, strong passwords must be used and they should never be shared.
    - Personal data should not be disclosed to unauthorized people, either within the company or externally.
    - Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
    - Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
- Data storage
    - These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller. When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

        - These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
            - When not required, the paper or files should be kept in a locked drawer or filing cabinet.
            - Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
            - Data printouts should be shredded and disposed of securely when no longer required.
        - When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:
            - Data should be protected by strong passwords that are changed regularly and never shared between employees.
            - If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
            - Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
            - Servers containing personal data should be sited in a secure location, away from general office space.
            - Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
            - Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
            - All servers and computers containing data should be protected by approved security software and a firewall.

- Data use
    - Personal data is of no value to <SHORT COMPANY NAME> unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:
        - When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
        - Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
        - Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.
        - Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

- Data accuracy
    - The law requires <SHORT COMPANY NAME> to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort <SHORT COMPANY NAME> should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
        - Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

        - Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
        - <SHORT COMPANY NAME> will make it easy for data subjects to update the information <SHORT COMPANY NAME> holds about them. For instance, via the company website.
        - Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
        - It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.
- Subject Access Requests
    - All individuals who are the subject of personal data held by <SHORT COMPANY NAME> are entitled to:
        - Ask what information the company holds about them and why.
        - Ask how to gain access to it.
        - Be informed how to keep it up to date.
        - Be informed how the company is meeting its data protection obligations.
- If an individual contacts the company requesting this information, this is called a subject access request.
- Subject access requests from individuals should be made by email, addressed to the data controller. The data controller can supply a standard request form.
- Individuals will be charged $<NN> per subject access request. The data controller will aim to provide the relevant data within <DD> days.
- The data controller will always verify the identity of anyone making a subject access request before handing over any information.
- Disclosing Data For Other Reasons
    - In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
    - Under these circumstances, <SHORT COMPANY NAME> will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

- Providing information
    - <SHORT COMPANY NAME> aims to ensure that individuals are aware that their data is being processed, and that they understand:
        - How the data is being used
        - How to exercise their rights
    - To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

5. Policy Compliance

- Compliance Measurement

The technology team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- Exceptions

Any exception to the policy must be approved in writing by management in advance detailing the methods/tactics, technologies, personnel, and systems scope of the request for approval.

- Non-Compliance

An employee or system user found to have violated this policy may be subject to disciplinary or legal action.

6. Related Standards, Policies, and Processes

None

7. Accountability and Responsibility

The <SHORT COMPANY NAME> IT manager is accountable for the maintenance and execution of this policy via the <SHORT COMPANY NAME> governance committee change management. It is the responsibility of all employees, contractors, consultants, temporary, and other workers at <SHORT COMPANY NAME> and its subsidiaries to adhere to this policy.

8. Acronyms and Definitions of Terms

Acronyms and Definition and terms can be found in the <SHORT COMPANY NAME>’s Glossary of Acronyms and Definition of Terms Document.

9. Revision History

Date of Change:

<EXAMPLE

11/14/2017 – Change Description>

Appendix A – References The following references illustrate public laws which have been issued on the subject of cyber security and should be used to demonstrate <SHORT COMPANY NAME> responsibilities associated with protection of its assets.