Policy # 002-2018.05 Data Protection Policy

Introduction

I5O Consulting Services needs to gather and use certain information about individuals.

This can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data will be collected, handled and stored to meet the company's data protection standards — and to comply with federal and state laws.

Why this policy exists

This data protection policy ensures I5O Consulting Services:

- Complies with data protection laws and follows good practices
- 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

Data Protection Law

The Data Protection Act 1998 describes how organizations — including I5O Consulting Services— must collect, handle and store personal information.

FERPA §§99.31. a.6 and 99.31.b.2 will govern work around higher education institution

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:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The head office of I5O Consulting Services
- All branches of I5O Consulting Services
- All staff and volunteers of I5O Consulting Services
- All contractors, suppliers and other people working on behalf of I5O Consulting Services
- 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
- …and any other information relating to individuals

Data Protection Risks

This policy helps to protect I5O Consulting Services from some very real data security risks, including:

Breaches of confidentiality

Failing to offer choice

Reputational damage

Responsibilities

- Everyone who works for or with I5O Consulting Services 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 **board of directors** is ultimately responsible for ensuring that I5O Consulting Services meets its legal obligations.

The **[data protection officer]** is responsible for:

- Keeping the board 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 people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data I5O Consulting Services 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/data scientist]** 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.

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 line managers.

I5O Consulting Services 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 I5O Consulting Services 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.
- Personal data should **never be transferred outside of the European Economic Area**.
- 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 I5O Consulting Services 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 I5O Consulting Services 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.
- I5O Consulting Services will make it **easy for data subjects to update the information** I5O Consulting Services 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 I5O Consulting Services 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 at: i5oconsultants@outlook.com.

The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 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, I5O Consulting Services 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.

Policy prepared by: Nancy Cotton

Approved by board / management on: May 30, 2018

Policy became operational on: May 30, 2018

Next review date: May 30, 2019