Data Protection Policy

Purpose

A Bright Solution must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

Scope

This data security policy applies all customer data, personal data, or other company data defined as sensitive by the company's data protect ion policy. *Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company IT services is also subject to this policy.*

Information that is classified as Public is not subject to this policy. Other data can be excluded from the policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.

Policy

A Bright Solution shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

General

- *Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.*
- *The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.*
- *Each user shall read this data security policy and the login and logoff guidelines and sign a statement that they understand the conditions of access.*
- *Records of user access may be used to provide evidence for security incident investigations.*

- *Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.*

Access Control Authorization

Access to company IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by the IT department based on records in the HR department.

Passwords are managed by the IT Service Desk. Requirements for password length, complexity and expiration are stated in the Data Protection Policy.

Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

Network Access

a. All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.

b. All staff and contractors who have remote access to company networks shall be authenticated using the VPN authentication mechanism only.

c. Segregation of networks shall be implemented as recommended by the company's network security research. Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation.

d. Network routing controls shall be implemented to support the access control policy.

User Responsibilities

a. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.

b. All users must keep their workplace clear of any sensitive or confidential information when they leave.

c. All users must keep their passwords confidential and not share them.

Application and Information Access

a. All company staff and contractors shall be granted access to the data and applications required for their job roles.

b. All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.

c. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

Access to Confidential, Restricted information

a. Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.

b. The responsibility to implement access restrictions lies with the IT Security department.

Technical Guidelines

Access control methods to be used shall include:

- *Auditing of attempts to log on to any device on the company network*
- *Windows NTFS permissions to files and folders*
- *Role-based access model*
- *Server access rights*
- *Firewall permissions*
- *Network zone and VLAN ACLs*
- *Web authentication rights*
- *Database access rights and ACLs*
- *Encryption at rest and in flight*
- *Network segregation*

Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

5. Reporting Requirements

a. Daily incident reports shall be produced and handled within the IT Security department or the incident response team.

b. Weekly reports detailing all incidents shall be produced by the IT Security department and sent to the IT manager or director.

c. High-priority incidents discovered by the IT Security department shall be immediately escalated; the IT manager should be contacted as soon as possible.

d. The IT Security department shall also product a monthly report showing the number of IT security incidents and the percentage that were resolved.

Ownership and Responsibilities

- ***Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.*

- ***Information Security Administrator** is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.*

- ***Users** include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees and volunteers.*

- ***The Incident Response Team** shall be chaired by an executive and include employees from departments such as IT Infrastructure, IT Application Security, Legal, Financial Services and Human Resources.*

Enforcement

This paragraph should state the penalties for access control violations.

Any user found in violation of this policy is subject to disciplinary action, up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection terminated.

Introduction

We hold personal data about our Employees, Clients, Suppliers and Service Providers (Data Subjects) for a variety of business purposes. This Policy sets out how we seek to protect personal data and ensure that Employees understand the rules governing their use of personal data to

which they have access in the course of their work. In particular, this Policy requires employees to ensure that the Data Protection Officer (DPO) (Mick Barrett) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

Responsibilities of the Office Manager:

- Addressing Data Protection queries from Clients, Sub-Contractors or Employees
- Coordinating with the DPO to ensure all marketing initiatives adhere to Data Protection laws and the company's Data Protection Policy
- Keeping the board updated about Data Protection responsibilities, risks and issues
- Reviewing all Data Protection procedures and Policies on a regular basis
- Answering questions on Data Protection from Employees and other stakeholders
- Responding to individuals such as Clients and Employees who wish to know which data is being held on them by A Bright Solution Ltd.

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

The Privacy Statement

- Sets out the purposes for which we hold personal data on Clients
- Highlights that our work may require us to give information to third parties such as business professionals
- Provides that Clients have a right of access to the personal data that we hold about them

Sensitive personal data

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 (e.g. to comply with legal obligations to ensure health and safety at work).

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Office Manager so that they can update your records.

Data security

We must keep personal data secure against loss or misuse.
Storing data securely

In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.

Printed data should be shredded when it is no longer needed
Data stored on a computer should be protected by strong passwords that are changed regularly.

We encourage all Employees to use a password manager to create and store their passwords.
Data stored on CDs or memory sticks must be locked away securely when they are not being used

The DPO must approve any cloud used to store data
Servers containing personal data must be kept in a secure location, away from general office space

Data should be regularly backed up in line with the company's backup procedures

Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must 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 that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Training

All A Bright Solution staff will receive training on this Policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our Policy and procedure.

Training is provided through a Toolbox Talk on a regular basis. It will cover:

- The law relating to Data Protection
- Our Data Protection and related Policies and Procedures.
- Completion of training is compulsory.
- Conditions for processing
- We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All Employees who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to Data Subjects in the form of a Privacy Statement.
- Justification for personal data
- We will process personal data in compliance with all six Data Protection principles.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject, but must also be by the permission of the individual.
Right to be forgotten

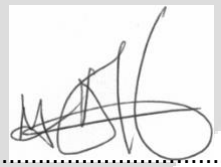
A Data Subject may request that any information held on them is deleted or removed.
Monitoring

Everyone must observe this Policy. The DPO has overall responsibility for this Policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this Policy very seriously. Failure to comply puts both you and the organisation at risk. 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 Head Office



Signed……
Mick Barrett
Director
8th August 2025

Signed……..
Sam Pailor
Director
8th August 2025