# Data Security 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.*

Signed.....
Mick Barrett
Director
8th August 2025

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