# ASSIGNMENT BRIEF AND FEEDBACK FORM

**104-175**

STUDENT No.

**Ms. Nalusamy Monapriya**

LECTURER:

**Network Security & Cryptography**

MODULE:

MODULE CODE:

**COM 411**

ASSIGNMENT NUMBER:

**1**

DATE HANDED OUT:

**1st August, 2025**

DATE DUE IN

**18th September , 2025**

ASSIGNMENT BRIEF

Create a cybersecurity policy for a small business that covers key areas, including:

* Data classification and protection
* Employee access control
* Password management
* Incident response procedures
* Compliance with regulatory requirements

STUDENT INSTRUCTIONS

1. This form must be attached to the front of your assignment.
2. The assignment must be handed in without fail by submission date (see assessment schedule for your course)
3. Ensure that submission date is date stamped by the reception staff when you hand it in.
4. Late submission will not be entertained unless with prior agreement with the tutor.
5. All assessable assignments must be word processed.

Contents

[ASSIGNMENT BRIEF AND FEEDBACK FORM 1](#_Toc209022617)

[**Cybersecurity Policy Notes – BrightPath Consulting** 3](#_Toc209022618)

[**1. Introduction** 3](#_Toc209022619)

[**2. Purpose** 3](#_Toc209022620)

[**3. Scope** 3](#_Toc209022621)

[**4. Data Classification & Protection** 3](#_Toc209022622)

[**4.1 Data Classification** 3](#_Toc209022623)

[**4.2 Protection Measures** 4](#_Toc209022624)

[**5. Employee Access Control** 4](#_Toc209022625)

[**6. Password Management** 4](#_Toc209022626)

[**7. Incident Response Procedures** 4](#_Toc209022627)

[**8. Regulatory Compliance** 5](#_Toc209022628)

[**9. Roles & Responsibilities** 5](#_Toc209022629)

[**10. Review & Maintenance** 5](#_Toc209022630)

[**11. Conclusion** 5](#_Toc209022631)

[Bibliography 6](#_Toc209022632)

**Cybersecurity Policy Notes – BrightPath Consulting**

**1. Introduction**

**BrightPath Consulting** is a growing digital services company that handles sensitive client data, intellectual property, and financial transactions. This Cybersecurity Policy is designed to safeguard the confidentiality, integrity, and availability of BrightPath’s information assets. It aligns with **ISO/IEC 27001:2013** and the **NIST Cybersecurity Framework (CSF)** to ensure a risk-based, industry-standard approach to security.

**2. Purpose**

The purpose of this policy is to:

* Protect company and client data against unauthorized access, disclosure, alteration, or destruction.
* Establish clear roles and responsibilities for employees and contractors.
* Ensure compliance with relevant regulations such as GDPR, Zambia’s Data Protection Act, and PCI-DSS (if handling cardholder data).
* Provide a framework for responding to cybersecurity incidents effectively.

**3. Scope**

This policy applies to:

1. All employees, contractors, and third-party vendors who access BrightPath’s IT systems, cloud platforms, or physical facilities.
2. All company-owned devices, networks, servers, cloud storage, and communication platforms.
3. All categories of data, including client information, employee records, and internal business data.

**4. Data Classification & Protection**

**4.1 Data Classification**

BrightPath classifies data into four categories:

1. **Public** – Marketing materials, website content (no restrictions).
2. **Internal** – Operational procedures, project templates (restricted to staff).
3. **Confidential** – Client data, contracts, financial reports (limited to authorized teams).
4. **Restricted** – PII, trade secrets, credentials (strictly controlled, encrypted).

**4.2 Protection Measures**

1. Encryption of confidential and restricted data both at rest (AES-256) and in transit (TLS 1.3).
2. Daily automated backups stored securely offsite with access limited to IT administrators.
3. Endpoint security software and firewalls deployed on all devices.
4. Physical security: locked server rooms, CCTV monitoring, visitor logs.

**5. Employee Access Control**

1. **Principle of Least Privilege (POLP):** Access rights are granted strictly based on job requirements.
2. Role-based access control (RBAC) implemented for cloud systems and internal tools.
3. Employee access is reviewed quarterly and revoked immediately upon termination or role change.
4. Third-party vendors sign NDAs and undergo security onboarding before system access.

**6. Password Management**

1. Passwords must be **minimum 12 characters** with a mix of uppercase, lowercase, numbers, and symbols.
2. **Multi-Factor Authentication (MFA)** required for email, VPN, cloud dashboards, and financial systems.
3. Passwords stored only in approved password managers — never in plain text.
4. Rotation every **180 days** or immediately after a suspected compromise.
5. Default passwords must be changed on first use.

**7. Incident Response Procedures**

1. **Identify:** Detect and confirm the incident.
2. **Contain:** Isolate affected systems.
3. **Eradicate & Recover:** Remove threat, restore clean backups.
4. **Post-Incident Review:** Root cause analysis, lessons learned, policy update.

High-severity incidents → notify clients/regulators immediately.

**8. Regulatory Compliance**

BrightPath adheres to:

1. **ISO/IEC 27001** controls for information security management.
2. **NIST CSF** categories: Identify, Protect, Detect, Respond, Recover.
3. **GDPR** for EU clients (lawful processing, data subject rights, breach notifications).
4. **Zambia’s Data Protection Act** (2021) for handling local PII.
5. **PCI-DSS** requirements if processing payment card data.

Compliance audits are conducted annually, and findings are reported to senior management.

**9. Roles & Responsibilities**

1. **Cybersecurity Lead:** Oversees policy, risks, compliance.
2. **IT Team:** System updates, patching, monitoring.
3. **Employees:** Follow policy, report incidents, attend training.
4. **Management:** Allocate budget and enforce compliance.

**10. Review & Maintenance**

This policy is reviewed **annually** or after a major security incident, technology change, or regulatory update. All changes are documented and communicated to staff.

**11. Conclusion**

By adopting this cybersecurity policy, BrightPath Consulting demonstrates its commitment to safeguarding sensitive data, maintaining client trust, and complying with international security standards. Every employee plays a vital role in upholding security best practices, thereby reducing the likelihood of breaches and ensuring business continuity.

# Bibliography

* *European Union (2016)* General Data Protection Regulation (GDPR) (EU) 2016/679. *Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (Accessed: 1 September 2025).*
* *Government of Zambia (2021)* Data Protection Act, No. 3 of 2021. *Lusaka: Government Printer.*
* *International Organization for Standardization (2013)* ISO/IEC 27001:2013 – Information Security Management Systems – Requirements. *Geneva: ISO.*
* *National Institute of Standards and Technology (2018)* Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Gaithersburg, MD: NIST. Available at:* [*https://www.nist.gov/cyberframework*](https://www.nist.gov/cyberframework) *(Accessed: 9 September 2025).*
* *PCI Security Standards Council (2022)* Payment Card Industry Data Security Standard (PCI DSS) v4.0. *Wakefield, MA: PCI SSC. Available at: https://www.pcisecuritystandards.org (Accessed: 17 September 2025).*
* *Center for Internet Security (2021)* CIS Critical Security Controls v8. *East Greenbush, NY: CIS. Available at: https://www.cisecurity.org/controls (Accessed: 13 September 2025).*
* *Verizon (2023)* Data Breach Investigations Report (DBIR). *Verizon Enterprise Solutions. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 14 September 2025).*