# ASSIGNMENT BRIEF AND FEEDBACK FORM

**104-175**

STUDENT No.

**MS. PRIYA**

LECTURER:

**NETWORK SECURITY**

MODULE:

MODULE CODE:

**COM 411**

ASSIGNMENT NUMBER:

**1**

DATE HANDED OUT:

**1st August, 2025**

DATE DUE IN

**20th September , 2025**

ASSIGNMENT BRIEF

**THEMES FOR PROJECT PREFERENCES**

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 stuff 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](#_Toc207280589)

[Cybersecurity Policy for Small Business 3](#_Toc207280590)

[Introduction 3](#_Toc207280591)

[Data Classification and Protection 3](#_Toc207280592)

[Employee Access Control 3](#_Toc207280593)

[Password Management 4](#_Toc207280594)

[Incident Response Procedures 4](#_Toc207280595)

[Compliance with Regulatory Requirements 4](#_Toc207280596)

[Conclusion 5](#_Toc207280597)

[References 6](#_Toc207280598)

# 

# Cybersecurity Policy for Small Business

## Introduction

In the digital era, small businesses face significant risks from cyber threats, including data breaches, malware attacks, phishing, and insider misuse. A cybersecurity policy is essential to protect business assets, ensure compliance with regulatory requirements, and build customer trust. This policy establishes guidelines for safeguarding information systems, managing employee access, and responding effectively to incidents. It aligns with the **NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover)** to provide structured and industry-recognised security practices (NIST, 2018).

## Data Classification and Protection

Business data shall be categorised into three classes:

1. **Confidential Data** – includes customer personal information, financial records, intellectual property, and trade secrets. Access is strictly limited to authorised personnel.
2. **Internal Use Data** – operational documents such as internal reports and business strategies. Access requires managerial approval.
3. **Public Data** – company information intended for public disclosure, such as marketing material and website content.

Confidential data must be encrypted both in transit and at rest using AES-256 encryption. Backups will be performed weekly and stored securely offsite or in a trusted cloud environment. Employees handling confidential information must sign non-disclosure agreements (ISO/IEC, 2013).

## Employee Access Control

Access to business systems will follow the **principle of least privilege**, ensuring employees only have access to the information necessary for their role. Role-based access control (RBAC) will be implemented for sensitive systems, and all administrative privileges must be approved by senior management. Access rights will be reviewed quarterly, and accounts of former employees will be disabled immediately upon termination. Multi-factor authentication (MFA) will be mandatory for remote access and administrative accounts (CIS, 2021).

## Password Management

Employees must use strong passwords with a minimum of **12 characters**, including uppercase, lowercase, numbers, and symbols. Passwords must not be reused across multiple systems and should be changed every 90 days. Password managers approved by the IT department will be provided to reduce the risk of weak or reused credentials. Default system passwords must be changed immediately upon installation. System monitoring will detect repeated failed login attempts, triggering account lockout after five unsuccessful tries (NIST, 2020).

## Incident Response Procedures

The business will adopt a **four-phase incident response plan**:

1. **Preparation** – Employees trained in recognising and reporting suspicious activity.
2. **Detection and Analysis** – All suspected incidents reported to the IT Security Officer within one hour. Logs will be analysed to verify the nature of the incident.
3. **Containment, Eradication, and Recovery** – Infected devices will be isolated, malware removed, and systems restored from backups.
4. **Post-Incident Review** – Lessons learned documented, and policies updated accordingly.

A communication protocol will be established to notify affected customers and regulatory bodies in the event of a breach, following relevant legal requirements such as the **General Data Protection Regulation (GDPR)** for personal data handling (European Commission, 2018).

## Compliance with Regulatory Requirements

The organisation is committed to complying with applicable legal and regulatory requirements, including:

* **GDPR (2018)** – protection of customer personal data for businesses handling EU citizens’ information.
* **Data Protection Act (2018, UK)** – guiding lawful data processing.
* **Local cybersecurity and privacy laws** within the jurisdiction of operation.

Compliance audits will be conducted annually, and employees will undergo mandatory training on data protection and security awareness. Any identified gaps will be addressed within 30 days.

# Conclusion

Cybersecurity is a shared responsibility across all levels of the business. By implementing structured policies based on the NIST Cybersecurity Framework, this small business can mitigate cyber risks, protect sensitive data, ensure regulatory compliance, and maintain trust with clients and stakeholders.

# References

* CIS (2021). CIS Controls v8: Prioritised set of Safeguards to Mitigate Cyber Attacks. Center for Internet Security.
* European Commission (2018). General Data Protection Regulation *(GDPR)*. Official Journal of the European Union.
* ISO/IEC (2013). ISO/IEC 27001: Information Security Management Systems – Requirements. International Organization for Standardization.
* NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology.
* NIST (2020). NIST Special Publication 800-63B: Digital Identity Guidelines. National Institute of Standards and Technology.