IT Security Standards Template

1. Document Control

Version	Date	Author	Description
1.0			Initial Draft

2. Purpose

Describe the purpose of this IT Security Standards document.

3. Scope

Define the scope (systems, departments, users, locations) covered by this document.

4. Roles and Responsibilities

Role	Responsibilities
IT Administrator	Maintain security configurations, monitor compliance, manage incidents.
End Users	Follow security policies, report incidents.

5. Security Standards

5.1 Access Control

- All users are assigned unique user IDs.
- Password policies enforce at least 8 characters, complexity requirements, and periodic changes.
- Access rights reviewed quarterly.

5.2 Physical Security

- Critical IT infrastructure must reside in secure, access-controlled locations.

5.3 Network Security

- Firewalls deployed and configured according to best practices.
- Regular network vulnerability assessments are conducted.

5.4 Data Protection

- Confidential data is encrypted at rest and in transit.
- Backups performed daily and tested monthly.

5.5 Incident Management

- Security incidents are reported promptly to responsible personnel.
- Incident response procedures are documented and reviewed regularly.

6. Compliance & Exceptions

All staff must comply with these standards. Any exceptions must be documented and approved by management.

7. Review & Revision

This document is reviewed annually or as required by changes in business or regulatory requirements.

8. References

- Company IT Security Policy
- ISO/IEC 27001
- NIST Cybersecurity Framework