Cybersecurity & IT Roles and Responsibilities Assignment Document

Organization Name: ______________________________
Effective Date: ______________________________
Review Cycle: ☐ Annual ☐ Semi-Annual ☐ As Needed

Purpose

This document formally assigns cybersecurity, IT, and data governance roles and responsibilities within the organization. Clear assignment and acknowledgment of these responsibilities supports the Confidentiality, Integrity, and Availability (CIA) of organizational systems and data.

Each role below includes a concise list of core responsibilities and a section for leadership assignment and acknowledgment by the Business Owner.

---

1. Security Administrator

Role Summary:
Responsible for implementing, maintaining, and reviewing security controls to protect the Confidentiality, Integrity, and Availability of company and customer data.

Key Responsibilities:

- Implement and configure security technologies and controls (e.g., endpoint protection, MFA, logging).
- Maintain compliance with internal security requirements and policies.
- Assist employees with security-related issues and questions.
- Perform ongoing reviews of security controls and recommend improvements.
- Monitor security alerts and coordinate response with other IT roles.

Assigned Individual:
Name: ____
Title: ____
Signature: _______________________________________
Date: ____

---

2. IT Systems Administrator

Role Summary:
Responsible for maintaining the functionality, performance, and availability of company hardware, software, and network systems.

Key Responsibilities:

- Install, maintain, and troubleshoot hardware, software, and network components.
- Provide real-time technical support to employees.
- Maintain system updates, patches, and configuration baselines.
- Document system configurations and technical procedures.
- Coordinate with the Security Administrator to ensure systems meet security standards.

Assigned Individual:
Name: ____
Title: ____
Signature: ____
Date: ____

---

3. Information Technology Manager

Role Summary:
Oversees IT and cybersecurity activities from a business and strategic perspective and serves as the liaison between technical staff and business leadership.

Key Responsibilities:

- Manage IT and cybersecurity budgets and resource planning.
- Draft, tailor, and approve IT and cybersecurity policies, plans, and procedures.
- Manage vendor relationships and third-party services.
- Oversee and prioritize IT and security initiatives.
- Report IT and cybersecurity risks and performance to business leadership.

Assigned Individual:
Name: ____

Title: ____
Signature: ____
Date: ____

---

4. Incident Response & Business Continuity Manager

Role Summary:
Responsible for preparing the organization to respond to, recover from, and continue operations during and after cybersecurity incidents or disruptions.

Key Responsibilities:

- Develop and maintain Incident Response, Disaster Recovery, and Business Continuity plans.
- Coordinate incident response activities during security events.
- Lead crisis communication and escalation efforts.
- Conduct incident response testing, tabletop exercises, and post-incident reviews.
- Collaborate with IT and Security staff to implement resilience improvements.

Assigned Individual:
Name: ____
Title: ____
Signature: ____
Date: ____

---

5. Data Owner

Role Summary:
Accountable for the protection, classification, and lifecycle management of specific datasets or departmental data.

Key Responsibilities:

- Classify and label data according to sensitivity and business impact.
- Define acceptable use, handling, and retention requirements for data.
- Approve access to data and review access periodically.

- Ensure data protection requirements are communicated to stewards and custodians.
- Accept accountability for data risk and impact in the event of compromise.

Assigned Dataset / Department: ____________________

Assigned Individual:
Name: ____
Title: ____
Signature: ____
Date: ____

---

6. Data Steward

Role Summary:
Responsible for maintaining data quality, consistency, and policy adherence under the direction of the Data Owner.

Key Responsibilities:

- Maintain data quality, accuracy, and standardization.
- Implement and monitor data handling and lifecycle workflows.
- Enforce data policies and standards defined by leadership.
- Coordinate with IT and Security roles on data-related initiatives.
- Support audits and reviews related to data governance.

Assigned Dataset / Function: ______________________

Assigned Individual:
Name: ____
Title: ____
Signature: ____
Date: ____

---

7. Data Custodian

Role Summary:
Responsible for implementing and operating the technical controls that protect organizational data.

Key Responsibilities:

- Implement access controls, encryption, and monitoring for data systems.
- Manage data storage platforms and backup/restore operations.
- Apply technical controls required by data policies and classifications.
- Monitor data systems for availability and integrity issues.
- Support incident response and forensic activities related to data systems.

Assigned Systems / Data Stores: ____________________

Assigned Individual:
Name: ____
Title: ____
Signature: ____
Date: ____

Business Owner Acknowledgment

I acknowledge that the above roles and responsibilities have been reviewed, assigned, and approved. I understand that I retain ultimate accountability for the cybersecurity and data protection posture of the organization.

Business Owner Name: _____________________________
Title: ____
Signature: _____________________________________
Date: ____

This document should be reviewed periodically and updated as business operations, technology, or staffing changes.