Incident Response Policy for Remote Access Breaches

1. Purpose

This policy outlines the procedures for identifying, reporting, and responding to remote access breaches to ensure the security and integrity of organizational systems and data.

2. Scope

This policy applies to all employees, contractors, and third-party users who access the organization's network and information systems remotely.

3. Definitions

- **Remote Access Breach:** Unauthorized access to systems or data via remote connections.
- **Incident Response Team (IRT):** Designated group responsible for managing security incidents.

4. Policy

1. **Monitoring:** All remote access attempts must be logged and monitored for abnormal activity.
2. **Identification:** Suspected remote access breaches must be identified promptly through:
    - Automated security alerts
    - User reports
    - Regular audits
3. **Reporting:** Any employee who detects or suspects a breach must report it immediately to the IRT.
4. **Containment:** Upon verification, the IRT will:
    - Disable compromised accounts or remote sessions
    - Restrict affected network segments
5. **Eradication:** IRT will remove unauthorized access vectors and ensure system integrity.
6. **Recovery:** Systems will be restored to normal operations after ensuring vulnerabilities are addressed.
7. **Notification:** Relevant internal stakeholders and, if required, external authorities will be notified as per regulatory requirements.
8. **Documentation:** All actions and findings will be documented for review and reporting.

5. Roles and Responsibilities

- **Employees:** Promptly report suspected breaches.
- **IRT:** Lead investigation, response, and documentation efforts.
- **IT Department:** Support containment, eradication, and recovery actions.

6. Review and Updates

This policy will be reviewed annually or after any major incident. Updates will be communicated to all parties concerned.

7. Approval

Approved by: _____ Date: _____