**Cybersecurity Incident Response Policy**

**Introduction**

**[Your Company Name] takes the security of our data and systems very seriously. This Cybersecurity Incident Response (CIR) Policy outlines the steps we will take to identify, contain, eradicate, and recover from cybersecurity incidents.**

**What is a Cybersecurity Incident?**

**A Cybersecurity Incident is any event that compromises the confidentiality, integrity, or availability of our data or IT systems. This includes, but is not limited to:**

* **Unauthorized access to systems or data**
* **Malware infections (viruses, ransomware)**
* **Phishing attacks**
* **Denial-of-Service attacks (DoS)**
* **Data breaches**
* **System outages**

**Reporting Procedures**

**All employees are obligated to report any suspected cybersecurity incidents immediately, regardless of severity. This includes:**

* **Unusual activity on your computer or network**
* **Suspicious emails or attachments**
* **Phishing attempts**
* **System errors or malfunctions**

**Reports can be made to the designated Incident Response Team (IRT) through:**

* **Email: [Insert Email Address Here]**
* **Phone: [Insert Phone Number Here] (Optional)**

**Incident Response Team (IRT)**

**The IRT is responsible for managing all aspects of a cybersecurity incident. This includes:**

* **Receiving and triaging incident reports**
* **Containing the incident (e.g., isolating infected systems)**
* **Eradicating the threat (e.g., removing malware)**
* **Recovering systems and data**
* **Investigating the incident to determine its cause and scope**
* **Reporting the incident to management and relevant authorities (if necessary)**

**Communication**

**The IRT will communicate with affected employees throughout the incident response process. This communication will include:**

* **Confirmation of the incident**
* **Actions being taken to address the incident**
* **Estimated timeframe for resolution**
* **Steps employees can take to mitigate any risks**

**Employee Responsibilities**

**All employees are expected to:**

* **Report suspected cybersecurity incidents immediately**
* **Follow instructions provided by the IRT during an incident**
* **Be aware of and follow company security policies (e.g., strong passwords, phishing awareness)**
* **Avoid clicking on suspicious links or attachments in emails**

**Revisions**

**This policy will be reviewed and updated periodically to reflect changes in technology and threats. Employees will be notified of any revisions.**

**Contact Information**

**If you have any questions about this policy, please contact your IT department or a member of the IRT.**