|  |
| --- |
| **RISK MANAGEMENT PLAN # 1**  Revision 0 Date: 4/2/2023  **System Name: Personal Mobile Phone** |
| **Risk Description and Consequences: Loss or theft of personal mobile phone.**  Threats: The phone can be lost or stolen.  Description: The personal mobile phone contains sensitive personal and work-related information. If the phone is lost or stolen, this information can be accessed and potentially used maliciously.  Consequence: The loss of personal and work-related information can lead to identity theft, data breaches, loss of confidential information, and reputational damage.  **Mitigation Strategies:**  What is being done to minimize the probability or consequence of the risk   1. Use a strong password or biometric authentication to lock the phone. 2. Install and keep up-to-date anti-theft software on the phone. 3. Regularly back up the data on the phone to a cloud or external storage device. 4. Avoid leaving the phone unattended in public places. 5. Do not use public Wi-Fi to access sensitive information.   **Contingency Actions and Trip Wires:**  Trip Wires/Indicators that the risk is happening  Actions to take upon identification that the risk is happening   1. If the phone is lost or stolen, immediately report it to the mobile service provider and local law enforcement. 2. If the phone is connected to a company account, immediately notify the company's IT department, and follow their instructions for reporting the incident.   **Resources needed:**  List all that are needed including: training, backups, software/hardware   1. Anti-theft software. 2. Cloud or external storage device. 3. Training on best practices for securing personal mobile devices.   **Notifications**  List contacts needed to be made should risk happen   1. Mobile service provider. 2. Local law enforcement. 3. Company IT department (if applicable).   **Subject Matter Expert/Person Responsible for implementing plan:**  Individual owner of the phone.  **Date Plan Must be Ready: 4/2/2023.**  **Approvals**  List all who need to approve the plan   1. Phone owner |
| **RISK MANAGEMENT PLAN # 2**  Revision 0 Date: 4/2/2023  **Asset Name: Company Database** |
| **Risk Description and Consequences: If the company's database is hacked, sensitive information could be compromised, potentially leading to loss of reputation, legal action, and financial damages.**  Threats: Cyber attacks, phishing scams, social engineering, etc.  Description: The company's database contains confidential information such as customer data, financial records, and employee information.  Consequence: If the database is hacked, it could lead to loss of data, loss of reputation, legal action, and financial damages.  **Mitigation Strategies:**  What is being done to minimize the probability or consequence of the risk   1. Regularly update software and security protocols to protect against new threats. 2. Conduct regular security audits and penetration testing to identify vulnerabilities. 3. Implement access controls to limit who can access the database. 4. Train employees on how to identify and prevent cyber threats. 5. Regularly backup data to minimize data loss in the event of an attack.   **Contingency Actions and Trip Wires:**  Trip Wires/Indicators that the risk is happening   1. Unusual activity on the network, such as multiple failed logins attempts or unauthorized access. 2. Reports of suspicious emails or other phishing attempts.   Actions to take upon identification that the risk is happening   1. Isolate affected systems to prevent further damage. 2. Notify IT security team and management. 3. Conduct a thorough investigation to determine the extent of the damage. 4. Notify customers and other affected parties if necessary. 5. Implement measures to prevent similar incidents in the future.   **Resources needed:**  List all that are needed including: training, backups, software/hardware   1. Cybersecurity software and hardware. 2. IT security personnel. 3. Employee training. 4. Backup systems.   **Notifications**  List contacts needed to be made should risk happen   1. IT security team. 2. Management. 3. Affected parties (if necessary).   **Subject Matter Expert/Person Responsible for implementing plan**  IT Security Manager  **Date Plan Must be Ready: 4/2/2023.**  **Approvals**  List all who need to approve the plan   1. IT Security Manager. 2. Director of IT. 3. CEO. |