# NIST CSF 2.0 Six Core Functions Mitigation for Assets

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset | Identify | Protect | Detect | Respond | Recover | Govern |
| Customer Data | Inventory and classify data. Assess risks. | Implement data encryption and access controls. | Monitor for unauthorized access or breaches. | Develop and test incident response plan. | Backup customer data regularly. Test recovery processes. | Data protection policy. |
| Network Systems | Identify network architecture and vulnerabilities. | Implement firewalls, intrusion prevention systems. | Monitor network traffic for anomalies. | Develop a network incident response strategy. | Restore network systems from backups. | Network security policy |
| Employee Accounts | Inventory employee accounts and access rights. | Enforce strong password policies and multi-factor authentication. | Monitor for unusual login patterns. | Respond to compromised accounts promptly. | Recover accounts and review access controls. | User account management policy |
| Financial Databases | Identify data classification and access levels. | Use encryption and limit access to authorized users. | Detect unauthorized access attempts. | Have a financial data breach response plan. | Restore financial databases from secure backups. | Database security policy. |
| Online Banking | Assess security measures and risks for online platforms. | Implement secure transaction protocols and encryption. | Monitor for suspicious transaction patterns. | Have a response plan for online banking incidents. | Review and update online banking security measures. | Online banking security policy |
| Mobile Banking Apps | Identify app vulnerabilities and risk factors. | Ensure apps are regularly updated and secure. | Monitor for app misuse and vulnerabilities. | Address mobile app security incidents. | Update apps and restore from secure versions. | Mobile banking security policy |
| Cloud Storage | Identify types of data stored and assess cloud provider risks. | Implement encryption and access controls for cloud data. | Monitor cloud storage for access anomalies. | Develop a response plan for cloud storage incidents. | Restore data from cloud backups if needed. | Cloud security governance |
| Third-Party Vendors | Assess third-party security practices and risks. | Ensure third-party agreements include security requirements. | Monitor third-party access and activities. | Respond to third-party breaches or incidents. | Review and update third-party security practices. | Third part risk management policy |
| Encryption Keys | Inventory and manage encryption key lifecycle. | Protect keys with secure storage and access controls. | Monitor for unauthorized access to keys. | Have a plan for compromised encryption keys. | Rotate and securely store encryption keys. | Key management policy.. |