Cybersecurity Policy

Kaiser Permanente

1. Organization and Stakeholder Management **2**

1.1 Communication of Cybersecurity Measures: 2

1.2 Compliance with Regulations: 2

1.3 Incident Communication: 2

2. Risk Management and Assessment **2**

2.1 Risk Assessment Process: 2

2.2 Regular Reviews and Updates: 2

3. Third-party and Supply Chain Management **3**

3.1 Vendor Reliability and Trust: 3

3.2 Continuous Monitoring: 3

4. Asset Management **3**

4.1 Identification of Critical Assets: 3

4.2 Asset Inventory: 3

5. Identity Management and Access Control **3**

5.1 Multi-Factor Authentication and Access Control: 3

5.2 Provisioning Accounts: 3

6. Application Security **3**

6.1 Configuration Management: 4

6.2 Data Backup: 4

7. Network Security **4**

7.1 Network Protection: 4

7.2 Least Functionality: 4

8. Incident Response **4**

8.1 Incident Handling and Reporting: 4

8.2 Coordination with Stakeholders: 4

9. Audit and Improvements **4**

9.1 Regular Audits: 4

9.2 Continuous Improvement: 5

10. Training **5**

10.1 Security Awareness and Training: 5

10.2 Role-based Training: 5

The Kaiser Permanente Cybersecurity policy is based primarily on security controls defined within the following:

- National Institute of Standards (NIST) Framework for Improving Critical Infrastructure Cybersecurity 2.0 (CSFW)

1. Organization and Stakeholder Management

Controls: GV.OC-02, GV.OC-03, RC.CO-03

1.1 Communication of Cybersecurity Measures:

Kaiser Permanente must communicate the importance of cybersecurity measures effectively to both internal and external stakeholders. This involves ensuring that stakeholders understand the significance of cybersecurity and fostering a culture of security awareness across the organization. Effective communication helps meet stakeholder expectations and ensures that everyone is aware of their roles in maintaining security.

1.2 Compliance with Regulations:

Healthcare organizations like Kaiser Permanente need to comply with regulations such as HIPAA and HITRUST. Understanding and managing these regulations are crucial for maintaining compliance and avoiding legal issues. Policies must be in place to ensure that all aspects of these regulations are adhered to and that staff are trained accordingly.

1.3 Incident Communication:

In the event of a cyber incident, sharing relevant information with all stakeholders is critical, as stipulated by control RC.CO-03. This ensures transparency and trust among stakeholders. The incident response plan must include clear communication protocols to notify stakeholders about incidents and the measures taken to address them.

2. Risk Management and Assessment

Controls: GV.RM-03, ID.RA-04

2.1 Risk Assessment Process:

The security team identifies threat sources, events, and vulnerabilities to assets. Regular vulnerability scans and penetration tests are conducted, prioritizing high-risk findings for remediation. This helps in assessing and mitigating risks effectively.

2.2 Regular Reviews and Updates:

Risk assessments are scheduled regularly to keep the risk management processes up-to-date. Any changes in the threat landscape or business processes should trigger a review of the risk management strategies to ensure they remain effective.

3. Third-party and Supply Chain Management

Controls: GV.SC-06, GV.SC-07, ID.IM-02, PR.AA-06, DE.CM-06

3.1 Vendor Reliability and Trust:

Kaiser Permanente must ensure that third-party contractors in supply chain operations, vendors, and national warehouse and logistics suppliers are reliable and trustworthy. This involves conducting thorough due diligence and risk assessments to verify the security practices of these third parties.

3.2 Continuous Monitoring:

Ongoing monitoring of third-party security practices is essential to ensure compliance with security requirements. Regular audits and assessments help identify any vulnerabilities or compliance issues that need to be addressed promptly.

4. Asset Management

Controls: ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-08, ID.RA-09

4.1 Identification of Critical Assets:

Performing risk assessments to identify critical assets is vital. This process helps in understanding the authenticity and integrity of these assets, allowing for better protection and management.

4.2 Asset Inventory:

Maintaining an accurate inventory of all physical resources, software, and external service providers is crucial. This includes cataloging all cloud services used by different products and teams, ensuring a comprehensive view of the assets.

5. Identity Management and Access Control

Controls: PR.AA-01, PR.AA-05, PR.IA-2, PR.IA-5, PR.AC-2, PR.AC-7

5.1 Multi-Factor Authentication and Access Control:

Protect critical assets and data by setting up multi-factor authentication and access control measures. This prevents unauthorized access and ensures that access policies are based on the principle of least privilege and separation of duties.

5.2 Provisioning Accounts:

Properly managing account provisioning to ensure that access is granted only to those who need it for their job roles. This helps in minimizing the risk of unauthorized access to sensitive information.

6. Application Security

Controls: PR.PS-01, PR.PS-04, PR.PS-06, PR.DS-11, RC.RP-03, RC.RP-05

6.1 Configuration Management:

Applications should be built with proper configuration management policies to ensure consistent security settings across all environments. This includes version control and regular updates to address any vulnerabilities.

6.2 Data Backup:

Regular backups of data log files should be performed to monitor performance throughout the software development life cycle. This helps quickly recover from any data loss incidents.

7. Network Security

Controls: ID.AM-03, PR.IR-01, DE.CM-01, DE.CM-06

7.1 Network Protection:

Implement controls to ensure network security, including monitoring and intrusion detection systems. This helps in identifying and responding to any security threats in a timely manner.

7.2 Least Functionality:

Access to tools and network resources should be granted as needed, using a least-privilege access model. This reduces the risk of unauthorized access or misuse of network resources.

8. Incident Response

Controls: ID.IM-04, DE.AE-08, RS.MA-01, RS.AN-06, RS.CO-02, RS.CO-03, RC.CO-03

8.1 Incident Handling and Reporting:

Develop and maintain an incident response plan to handle and report security incidents promptly and efficiently. This plan should include roles and responsibilities, communication protocols, and post-incident analysis.

8.2 Coordination with Stakeholders:

During an incident, coordination with security vendors, customers, suppliers, and internal team members is essential. This ensures a unified and effective response to mitigate the impact of the incident.

9. Audit and Improvements

Controls: ID.IM-02, ID.IM-03, DE.CM-06, DE.CM-09, AU-2

9.1 Regular Audits:

Conduct regular audits to ensure compliance with security policies and identify areas for improvement. Audits help in maintaining the effectiveness of security measures and addressing any gaps.

9.2 Continuous Improvement:

Based on audit findings and new threat intelligence, continuously improve security processes. This proactive approach helps in staying ahead of potential threats.

10. Training

Controls: PR.AT-01, PR.AT-02

10.1 Security Awareness and Training:

Provide ongoing security training and awareness programs to all personnel. This ensures that everyone understands their roles and responsibilities in maintaining security and is aware of the latest threats and best practices.

10.2 Role-based Training:

Tailor training programs to specific roles, especially for those handling personal data or sensitive information. This ensures that employees have the knowledge and skills required for their specific responsibilities.