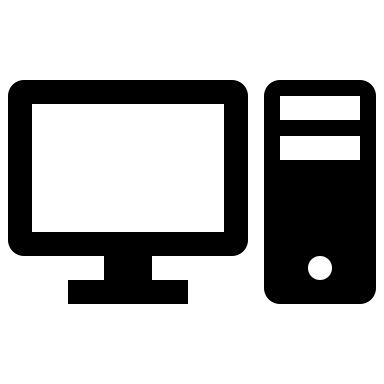
****

Jennifer Palmer

April 25, 2025

**Gennect Cybersecurity Risk Management Policy**

**1. Asset ManagementGennect Cybersecurity Risk Management Policy**

**1.1 Inventory of Assets**

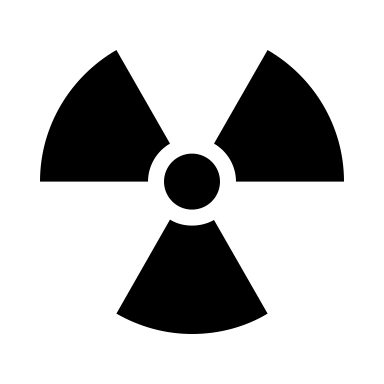
* **Inventory List**: We maintain an up-to-date inventory of all physical and digital assets, including servers, workstations, mobile devices, software applications, and data repositories. Current list as of 4/25/2025:
  + - **Servers**: 10 physical servers, 5 virtual servers
    - **Workstations**: 150 desktops, 50 laptops
    - **Mobile Devices**: 30 tablets, 20 smartphones
    - **Software Applications**: Microsoft Office Suite, Adobe Creative Cloud
    - **Data Repositories**: Customer database, financial records

**1.2 Asset Protection**

* **Security Measures**: We implement appropriate security measures to protect assets from unauthorized access, theft, and damage. In place are the following:
  + - **Encryption**: AES-256 encryption for sensitive data
    - **Access Controls**: Role-based access control (RBAC) for critical systems
    - **Physical Security**: Secure server rooms with biometric access

**1.3 Asset Disposal**

* **Disposal Procedures**: We follow procedures for the secure disposal of assets, ensuring that sensitive data is irrecoverable.
  + - **Data Wiping**: Use software tools to securely wipe data from hard drives
    - **Physical Destruction**: Shred or crush hard drives before disposal
    - **Documentation**: Maintain records of disposed assets and methods used

**2. Risk Assessment**

**2.1 Risk Identification**

* **Risk Identification Process**: We monitor for potential cybersecurity risks to the organization’s assets, operations, and individuals using threat intelligence and historical data.
  + - **Threat Intelligence**: We regularly review reports from cybersecurity firms
    - **Historical Data**: We analyze past incidents and breaches

**2.2 Risk Analysis**

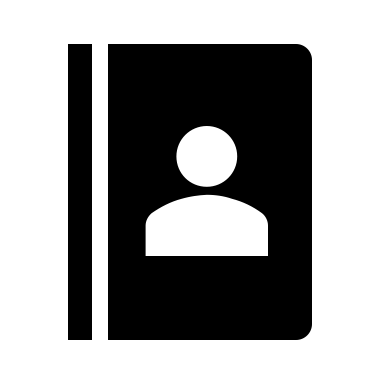
* **Risk Analysis Methodology**: We assess the likelihood and impact of identified risks, prioritizing them based on their potential impact on the organization.
  + - **Likelihood**: High, Medium, Low
    - **Impact**: Critical, Major, Minor

**2.3 Risk Mitigation**

* **Mitigation Strategies**: We develop and implement strategies to mitigate identified risks such as:
  + - **Patch Management**: We regularly update software and systems
    - **Network Segmentation**: We separate sensitive data from general network traffic
    - **Employee Training**: We conduct regular cybersecurity awareness sessions

**2.4 Risk Monitoring**

* **Continuous Monitoring**: We continuously monitoring for new and evolving risks, adjusting risk management strategies as necessary based on monitoring results.
  + - **Monitoring Tools**: We use SIEM (Security Information and Event Management) systems
    - **Adjustments**: We update firewall rules based on new threat patterns

**3. Access Control**

**3.1 Access Management**

* **Role-Based Access Control**: We implement role-based access control (RBAC) to ensure users have appropriate access levels, regularly reviewing and updating access permissions.
  + - **Roles**: Admin, User, Guest
    - **Permissions**: Admins have full access, Users have limited access, Guests have minimal access

**3.2 Authentication**

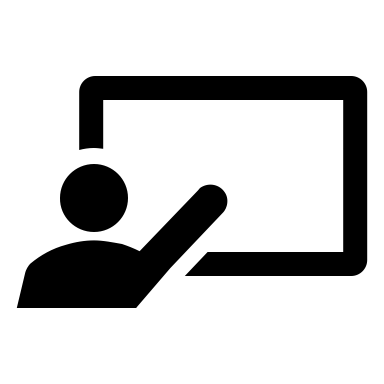
* **Multi-Factor Authentication**: We use multi-factor authentication (MFA) for accessing sensitive systems and data, ensuring authentication mechanisms are robust and regularly updated.
  + - **MFA Methods**: SMS, email, and app-based authentication
    - **Update Frequency**: Quarterly reviews of authentication methods

**3.3 Authorization**

* **Authorization Protocols**: We stablished clear authorization protocols for accessing critical systems and data, documenting and auditing authorization processes.
  + - **Protocols**: Approval from department heads for access requests
    - **Audits**: Monthly audits of access logs

**3.4 Access Review**

* **Regular Access Reviews**: We conduct regular access reviews to ensure compliance with access control policies, removing or adjusting access permissions as necessary based on review findings.
  + - **Review Frequency**: Bi-annual access reviews
    - **Adjustments**: Revoke access for terminated employees

**4. Awareness and Training**

**4.1 Employee Training**

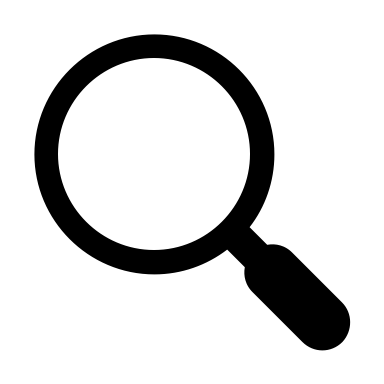
* **Cybersecurity Training**: We provide regular cybersecurity training to all employees, ensuring training covers current threats, best practices, and organizational policies.
  + - **Training Topics**: Phishing, password management, data protection
    - **Frequency**: Quarterly training sessions

**4.2 Awareness Programs**

* **Ongoing Awareness Programs**: We implement ongoing awareness programs to keep cybersecurity top-of-mind for employees using various methods such as newsletters, workshops, and simulations.
  + - **Methods**: Monthly newsletters, annual workshops, quarterly phishing simulations

**4.3 Incident Response Training**

* **Incident Response Training**: We train employees on how to respond to cybersecurity incidents, conducting regular drills and simulations to test incident response readiness.
  + - **Drills**: Annual incident response drills
    - **Simulations**: Quarterly tabletop exercises

**5. Security Continuous Monitoring**

**5.1 Monitoring Systems**

* **Deployment of Monitoring Systems**: We deploy monitoring systems to continuously track network and system activity, ensuring monitoring systems are capable of detecting anomalies and potential threats.
  + - **Tools**: SIEM systems, intrusion detection systems (IDS)
    - **Capabilities**: Real-time alerting, anomaly detection

**5.2 Incident Detection**

* **Detection Protocols**: We establish protocols for the timely detection of cybersecurity incidents using automated tools and manual processes to identify incidents.
  + - **Tools**: Automated threat detection software
    - **Processes**: Manual log reviews

**5.3 Incident Response**

* **Incident Response Plan**: We develop and implement an incident response plan, ensuring the plan includes steps for containment, eradication, recovery, and post-incident analysis.
  + - **Steps**:
      * **Containment**: Isolate affected systems
      * **Eradication**: Remove malicious code
      * **Recovery**: Restore systems from backups
      * **Post-Incident Analysis**: Review incident to improve future response

**5.4 Reporting and Analysis**

* **Regular Reporting**: We regularly report on monitoring results and incident responses, analyzing reports to identify trends and improve security measures.
  + - **Reports**: Monthly security reports
    - **Analysis**: Trend analysis to identify recurring issue