**Policies for MSPEI**

**1. Software and Downloads Policy:** To maintain the security of our healthcare systems and data, please refrain from downloading any software, applications, or files onto the system without prior authorization from the IT department. Unauthorized downloads may introduce vulnerabilities and compromise the integrity of our network.

**2. Password Confidentiality Policy:** To ensure the confidentiality and security of your account, it is imperative that you do not share your password with any other team member. Passwords are personal and should only be used by the assigned user.

**3. Device Connection Policy:** To prevent potential security risks, please avoid connecting any external USB drives or other devices to the MSPEI network system without obtaining explicit permission from the IT department. Unauthorized devices may introduce malware or unauthorized access points.

**4. Termination and Access Removal Policy:** Upon joining our team, each staff member acknowledges having read and agreed to our information security policies. In the event of a staff member's departure, whether through resignation or termination, it is crucial to promptly revoke all system access to maintain the security and confidentiality of our healthcare operations.

Please note that the commitment to protect sensitive information remains in effect even after leaving the company. Legal action may be pursued against individuals who disclose sensitive information to unauthorized parties, regardless of their employment status.

Your compliance with these policies plays a vital role in upholding the trust and integrity of our healthcare group's operations and ensuring the safeguarding of patient data.

**5. Password Security and Rotation Policy:** To enhance the security of our systems and protect patient data, all passwords must adhere to the following guidelines:

* Passwords must be changed every 90 days.
* Passwords must be a minimum of 12 characters in length.
* Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters.

These policies aim to ensure the security and confidentiality of our healthcare group's systems and data. It is essential that all staff members adhere to these guidelines to maintain the integrity of our operations and safeguard patient information.

\

**Procedures for MSPEI**

1. **Policy Reference:** *Software and Downloads Policy*
2. **Objective:** To maintain the security of healthcare systems and data by preventing unauthorized software downloads that may compromise network integrity.
3. **Procedure:** a. All staff members must refrain from downloading any software, applications, or files onto MSPEI systems without prior authorization from the IT department. b. To request software or application downloads, staff members must submit a formal request to the IT department, outlining the necessity and purpose of the software. c. The IT department will evaluate the request and grant authorization if the software aligns with MSPEI's security and compatibility standards. d. Unauthorized software downloads are strictly prohibited and may result in disciplinary actions.

**Procedure: Password Confidentiality and Security**

1. **Policy Reference:** Password Confidentiality Policy
2. **Objective:** To ensure the confidentiality and security of user accounts and prevent unauthorized access.
3. **Procedure:** a. All staff members are responsible for maintaining the confidentiality of their passwords and not sharing them with others. b. Passwords should be complex and adhere to the guidelines outlined in the Password Security and Rotation Policy. c. In case of suspected compromise or unauthorized access, staff members must promptly report the incident to the IT department. d. Passwords should not be stored in easily accessible locations or shared electronically.

**Procedure: Device Connection and Access Authorization**

1. **Policy Reference:** Device Connection Policy
2. **Objective:** To prevent potential security risks by controlling external device connections to MSPEI network systems.
3. **Procedure:** a. Staff members must seek explicit permission from the IT department before connecting any external USB drives or devices to MSPEI network systems. b. To request device connections, staff members should submit a request to the IT department, specifying the purpose and details of the connection. c. Unauthorized device connections are prohibited to prevent the introduction of malware or unauthorized access points. d. The IT department will evaluate the request and grant authorization based on security considerations.

**Procedure: Termination and Access Revocation**

1. **Policy Reference:** Termination and Access Removal Policy
2. **Objective:** To ensure the security and confidentiality of healthcare operations by promptly revoking system access upon staff departure.
3. **Procedure:** a. Upon staff departure, whether through resignation or termination, the HR department will promptly notify the IT department. b. The IT department will immediately revoke the departing staff member's system access and credentials to prevent unauthorized access. c. Access revocation will be thorough, including email accounts, network access, and other relevant systems. d. Revoked access will be documented and logged for future reference and auditing.

**Procedure: Password Security and Rotation**

1. **Policy Reference:** Password Security and Rotation Policy
2. **Objective:** To enhance system security by ensuring strong and regularly rotated passwords.
3. **Procedure:** a. All staff members must adhere to the guidelines outlined in the Password Security and Rotation Policy. b. Passwords must be changed every 90 days. c. Passwords must be a minimum of 12 characters in length and include a combination of uppercase letters, lowercase letters, numbers, and special characters. d. Passwords must not be reused for a minimum of six password changes. e. IT department will enforce password rotation and complexity requirements.

These procedures align with the mentioned policies and emphasize the importance of data security and protection within MSPEI's healthcare operations. The implementation of these procedures, in conjunction with the cybersecurity playbook, will contribute to safeguarding patient data, maintaining operational integrity, and effectively responding to potential data theft incidents.