Cymbal Bank: Risk Management Policy

Purpose: This policy has been created to identify, assess, and manage risks associated with Cymbal Bank's use of hybrid cloud solutions. This policy includes guidelines to ensure the confidentiality, integrity, and availability of Cymbal Bank's cloud resources.

1. Access Control
    - If an employee expects to leave their workstation unattended, they must lock their workstation. Employee workstations may not be configured to automatically lock.
    - Privileged functions include access to sensitive data and the ability to modify system configurations, such as security settings. Privileged functions can be carried out by non-privileged accounts, if necessary.
2. Awareness and Training
    - New employees will be trained on current cyber threats.
    - All new employees must receive identical cyber threat training, regardless of their role.
3. Configuration Management
    - All users can install software on their work devices, as necessary.
    - Before system changes are implemented, they should be analyzed for their potential security impacts.
4. Identification and Authentication
    - User passwords are required to be complex and must be changed regularly. User passwords may not contain spaces or punctuation.
    - Maintain a list of commonly used, expected, or compromised passwords and update the list once per month. When a user attempts to change their password, verify that the new password is not on the list.
5. Incident Response
    - Employees whose responsibilities are part of incident response should receive incident response training within one week of assuming those responsibilities. More training should be conducted every three months or as required by system changes, and the training content should be updated each year.
    - Incident response training should include simulated incidents to facilitate employees practicing their responsibilities.
6. Physical and Environmental Protection
    - The security team must develop and maintain a list of individuals who are authorized to access Cymbal Bank's server room. These individuals must be

granted authorization credentials and cannot be removed from the list once added.
    - In order to access the server room, visitors must provide two forms of identification from the approved list.
7. Risk Assessment
    - The security team must determine the current cyber threat environment on an ongoing basis using security newsletters and cyber threat databases.
    - The security team monitors and scans for vulnerabilities in the cloud environment.
8. System and Information Integrity
    - Cymbal Bank uses centrally managed identity verification tools to verify employee and user identity.
    - Security alert and advisory information should be shared throughout the security team on a regular basis.