Segon-Marill Cyber Security Policies

1. **Access control policy:** Segon-Marill International Movers Plc. specified role-based access control (RBAC) within an organization. Based on this staffs of the company privileged with:
   - Administrative access
   - Operational Access
2. **Incident response policy:** The company conducts the following activities during occurrence of cyber security incidents:
   - Identifying the source
   - Eradication of the incident (removing the malicious software and cleaning up the system)
   - Recovery of system and data
   - Communication and reporting
   - Post incident reviews and improvement
3. **Password policy:** There is established guidelines for creating and managing passwords within the company. Accordingly:
   - Minimum password length 8 character
   - Maximum password age 6 months
   - Complexity requirements: at least one upper case, one lower case, one number and one special character
   - Password must be changed after any administrative changes
   - Two-factor authentication (2FA) required for login
   - Password sharing is prohibited
   - Password should not include any personal information such as name, age, phone numbers, birthdate etc.
   - Provide user education and awareness training on password security best practices
4. **Data classification policy:** we have outlined how data should be classified and handled based on its sensitivity. Accordingly:
   - Confidential: PII, financial records, trade secrets
   - Private: employee records, internal communications
   - Public: press release, company brochures, all information in our website
   - Restricted (for specific audiences only): legal documents, researches
   - Top secret: intelligence data
5. **Remote access policy:** We have defined the conditions under which employees can access company resources from outside the office. Accordingly:

- Employees are requested two-factor authentication (must provide two form of identification, password and finger print or security token) before being granted access to remote systems.
- Network segmentation: staffs do not access sensitive data outside of the Segon environment
- Remote access software: we use specialized software to control and monitor remote access to systems and data (auditing of user's activity).
- Remote wipe: the company established a system to remotely delete all data from a device that has been lost or stollen

6. **Acceptable use policy:** The company outlined the acceptable and prohibited uses of company equipment and network resources. Accordingly:
   - Prohibiting the unauthorized access or use of networks, applications and systems
   - Prohibiting the use of the network or system for illegal activities
7. **Encryption policy:** The company specified the types of data that must be encrypted and the encryption methods to be used. Accordingly:
   - Data to be encrypted: PII, financial data, strategic plan
   - Encryption method used: symmetric encryption (AES) and Transport Layer Security (TLS) to encrypt data in transit.
8. **Data retention and disposal policy:** We have determined how long data should be retained and the procedures for securely disposing of it. Accordingly:
   - Retaining customer data for at least 5 years
   - Retaining financial data as set out in the applicable law
   - Securely wiping or destroying old backups or servers that are retired
9. **Third-party vendor management policy:** We have outlined the security requirements for working with vendors and service providers. Accordingly, we assess the vendors'
   - Cyber security policies
   - Due diligence
   - Incident response plan
10. **Continuity of operations plan:** The company committed to re-operate the business process after occurrence of cyber incident through taking appropriate correction and corrective actions