ALAGO CHIEMELA VICTOR

Company Name: BetterTech Solutions, Inc.

Security Policies:

1. **Access Control Policy**
    - All employees should have role-based access to company resources.
    - Access to sensitive data should be restricted to authorized personnel.
    - Regular access reviews should be conducted.
2. **Password Policy**
    - Passwords must be a minimum of 12 characters and include a mix of letters, numbers, and symbols.
    - Passwords must be changed every 90 days.
    - Two-factor authentication (2FA) is mandatory for accessing company systems.
3. **Data Encryption Policy**
    - All sensitive data in transit and at rest must be encrypted.
    - Data encryption should follow industry standards and best practices.
4. **Incident Response Policy**
    - A documented incident response plan should be in place.
    - Employees should report security incidents promptly.
    - An incident response team should be designated.
5. **BYOD (Bring Your Own Device) Policy**
    - Employee-owned devices should meet security standards.
    - Mobile device management (MDM) software should be used to secure mobile devices.
6. **Remote Work Policy**
    - Remote work is allowed with prior authorization.
    - Employees must use secure VPNs and follow security protocols when working remotely.

7. **Physical Security Policy**
    - Access to company premises should be restricted to authorized personnel.
    - Visitors should be logged and provided with visitor badges.
8. **Data Backup and Recovery Policy**
    - Regular data backups should be performed and tested (every 8 working hours)
    - A disaster recovery plan should be in place.
9. **Social Engineering Awareness Policy**
    - Employees should be trained to recognize and report social engineering attempts.
    - Regular awareness training sessions should be conducted.
10. **Vendor Security Policy**
    - Vendors should meet security and data privacy standards.
    - Contracts with vendors should include security and data protection clauses.
11. **Data Classification and Handling Policy**
    - Data should be classified based on its sensitivity (e.g., public, internal, confidential, highly confidential).
    - Access and handling of data should align with its classification.
    - Data classification should be reviewed periodically.
12. **Software and Patch Management Policy**
    - All software and applications should be regularly updated with security patches.
    - Vulnerability assessments and patch management processes should be in place.
    - Only authorized personnel should be allowed to install or update software.

Departments Structure

1. **Executive Team**
    - Chief Executive Officer (CEO)
    - Chief Financial Officer (CFO)
    - Chief Technology Officer (CTO)
    - Chief Operating Officer (COO)
    - Total Employees: 4

2. **Human Resources & Management**
    - Human Resources Manager
    - Talent Acquisition Specialist
    - Employee Relations Specialist
    - Training and Development Manager
    - Total Employees: 4

3. **Technical Department**
    - Development Team (Developers, Engineers)
    - IT Support Team
    - Database Administrators
    - Network Administrators
    - Total Employees: 25

4. **Sales and Marketing**
    - Sales Team (Sales Representatives, Account Managers)
    - Marketing Team (Marketing Specialists, Graphic Designers)
    - Total Employees: 15

5. **Finance Department**
    - Accounting Team (Accountants, Bookkeepers)
    - Financial Analysts
    - Total Employees: 7

6. Research and Development (R&D) Department

- Research Scientists
- Product Development Engineers
- Quality Assurance Testers
- Total Employees: 10

7. Customer Support Department

- Customer Support Representatives
- Technical Support Specialists
- Customer Support Managers
- Total Employees: 12