Company Data Security Policy

1. **Access Control**: Access to personal and sensitive data is restricted to authorized employees only, with strict access levels based on job roles.
2. **Encryption**: All sensitive data, including personal information, is encrypted both in transit and at rest.
3. **Regular Audits**: We conduct periodic security audits to identify and mitigate vulnerabilities in our data systems and infrastructure.
4. **Incident Response**: In case of a data breach, we have a response plan in place to contain the breach, notify affected parties, and take corrective actions.
5. **Third-Party Security**: Vendors with access to our data are vetted for compliance with our security standards, including data encryption and restricted access protocols.