IT Compliance Agreement for using AI

Data Classification Policy

Company data is classified into three levels: Public, Internal, and Confidential. Public data can be shared externally. Internal data is for company use only. Confidential data requires special handling and encryption. All new data must be classified within 24 hours of creation.

LLM Usage Compliance

All Large Language Model usage must be approved by the IT Security team within 48 hours of request. Employees must not input confidential company data into public LLM services. Approved LLM tools must be logged and monitored. All LLM-generated content must be reviewed for accuracy within 24 hours before use.

AI Content Generation Policy

AI-generated content must be clearly labeled as such. Employees using AI tools for content creation must verify factual accuracy within 48 hours. No sensitive customer or business data can be processed through AI tools without explicit approval within 72 hours. All AI usage must be documented within 24 hours of use.

Access Control Standards

User access is granted based on job role and follows the principle of least privilege. Access reviews are conducted quarterly by the 30th of March, June, September, and December. Terminated employees have their access revoked immediately upon departure. Access requests must be approved within 3 business days.

Compliance Monitoring

Regular audits are conducted to ensure compliance with all IT policies. Non-compliance issues are addressed within 30 days of discovery. Annual training is required for all employees on security policies and procedures by December 31st each year. Compliance reports are due quarterly by the 15th of each quarter.