Generative Consulting

Generative AI Policy Template (Cybersecurity Addendum)

https://generativeconsulting.ai

Your organization is represented in this template as “ABC”. Simply replace this stand-in with your organization’s information to use this template. You can safely remove this page.

Gen AI Policy Template - Cybersecurity Addendum

Gen AI Implementation and Integration Guidelines

1. **Where possible, locally hosted versions of Gen AI should be used, particularly with respect to the efficient mining of internal data. Separation of Gen AI models may be necessary or advisable for different use cases. In all use cases, for both hosted versions and cloud-based Gen AI platforms, ensure sign-off of all Gen AI output by the designated Risk and Compliance team.**
2. **Use Gen AI technology responsibly ensuring compliance with applicable laws and regulations, conducting risk impact assessments and regulatory reviews, and considering the potential impact on stakeholders. Prepare awareness campaigns and ongoing training for employees.**
3. **Identify any technology, infrastructure, or business processes reliant on Gen AI, implement appropriate safeguards or controls, log and archive all Gen AI usage according to applicable laws and regulatory requirements.**
4. **Identify all data, intellectual property, integrations, internal and external applications, and services that a Gen AI application might have access to. Implement proper security and access controls, providing the minimal access necessary for the Gen AI application to perform its tasks.**

https://generativeconsulting.ai

5. When building Gen AI integrations, evaluate and curate the appropriate providers by functionality and quality control. In conjunction with necessary advisors and legal resources, consider the regulatory context and requirements for audits and compliance; identify any risks to intellectual property; validate output for accuracy free from inaccurate or fabricated answers, biases or hallucinations, and; review protocols for data breach potential.
6. Ensure that the Legal and Compliance team reviews Gen AI output for any potential legal violations in a review schedule to be determined.

Violations of Gen AI usage policies may result in disciplinary action, up to and including termination of employment.

Generative AI Security Checklist

- **Risk Assessment:** **Conduct a comprehensive risk assessment for the use of Gen AI technologies, considering potential threats, vulnerabilities, and impacts.**
- **Data Privacy:** **Ensure that the use of Gen AI complies with all relevant data privacy laws and regulations. This includes the GDPR of the EU, the CCPA, or any other applicable regional or sector-specific regulations.**
- **Data Access Control:** **Implement strict access controls to ensure that Gen AI technologies can only access the data they need to function and nothing more.**
- **Third-Party Risk Management:** **If using third-party Gen AI technologies, conduct a thorough review of the provider's security practices and ensure they meet your organization's standards.**
- **Security Measures:** **Implement appropriate security measures to protect against unauthorized access to Gen AI technologies. This could include encryption, secure coding practices, and regular security testing.**
- **Monitoring and Logging:** **Establish a system for monitoring and logging all interactions with Gen AI technologies. This can help detect any unusual or suspicious activity and provide an essential audit trail.**
- **Data Anonymization:** **Ensure that all company and other sensitive data is removed from any prompt requests and confirm with human-in-the-loop review of Gen AI output both for internal and external use.**

- **Incident Response Plan:** **Develop an incident response plan that specifically addresses potential security incidents involving Gen AI technologies.**
- **Employee Training:** **Provide regular training to employees on the secure use of Gen AI technologies, including familiarity with the Gen AI Policy of ABC. This should include guidance on what information can and cannot be shared with Gen AI technologies, human monitoring and data anonymization.**
- **Regular Audits:** **Conduct regular audits of your Gen AI technologies and their use to ensure compliance with the Policy and to identify any potential security issues.**
- **Review and Update:** **Regularly review and update your Gen AI Policy and security checklist to ensure they remain relevant as technology and associated threats evolve.**

Please note that this "Cybersecurity Addendum" and the related Gen AI Policy are templates only and will need to be tailored to fit the specific needs and circumstances of your organization. Always consult with a legal professional when drafting policies to ensure compliance with all relevant laws and regulations. Always consult with a security professional when developing security checklists to ensure they adequately address all potential risks.

The content here is for informational purposes only and does not constitute tax, business, legal nor investment advice. Protect your interests and consult your own advisors as necessary.

https://generativeconsulting.ai