# INFORMATION SECURITY AND DATA PRIVACY POLICY

Ambac recognizes the importance of data security. The security of our systems is essential to our company and to our clients. We have instituted technical measures, and adopted policies and procedures, designed to implement cybersecurity safeguards to protect our technology systems and the confidentiality, integrity and availability of information stored and processed on those systems. We are committed to adapting our network security to mitigate the risks of online threats to our systems and data.

## Governance and Management of Data and Information Security

Ambac's Information Security Program (the "Program") builds on multiple years of focus on three essential components: people, processes and technology. By combining the expertise of our people, processes and advanced technology, the company has implemented an information security program designed to defend against cyber threats and to quickly respond to prospective and identified risks.

## Data and Information Oversight

Ambac has established a Data Governance Committee (DGC), which includes members of the company's Senior Management Team, including the Chief Executive Officer, Chief Operating Officer, General Counsel, Chief Compliance Officer, and Chief Financial Officer.

The DGC is responsible for overseeing the development and implementation of Ambac's data management framework, which includes the development of policies, processes, and measures to manage information and data across the enterprise and its businesses, and to establish practices to protect the security of information and the privacy of individuals, in compliance with applicable security and privacy laws and regulations.

Ambac's information security functions are monitored and managed using a top-down approach, starting with the Board of Directors, and similarly overseen by the Chief Operating Officer, General Counsel and Chief Compliance Officer. Information security risk is included in the Enterprise Risk Management presentations to the Board. The Board receives periodic updates on information security risks from the Chief Information Security Officer (CISO) and status of compliance with applicable information security laws and regulations from the Deputy Compliance Officer, Privacy and Information Security (Deputy Compliance Officer). The CISO and Deputy Compliance Officer also report regularly on adherence to compliance requirements, including applicable US security and privacy regulations and industry requirements.

## Information Security and Risk Mitigation Programs

Ambac's information security program demonstrates our commitment to protecting information, systems and people across the enterprise. Information is a critical and essential asset to Ambac's business and the information security program is designed to maintain the confidentiality, integrity and availability of our information systems and data.

Our processes focus on the five steps of industry best practice for cybersecurity: identify, protect, detect, respond, and recover, as set by the U.S. National Institute of Standards and Technology (NIST). Additionally, the program includes applicable state legal and regulatory requirements. The program sets out the information security requirements and expectations to which employees, third party providers, and adopted technology solutions must comply.

Ambac's information security program is designed to reduce data security risk by the use of security technologies and processes in several areas. The Program includes risk mitigating efforts such as:

- **Implementing, managing and maintaining the security technologies and processes that are designed to protect information systems and data, such a multifactor authentication for remote access to system applications;**
- **Implementing technologies and processes to regularly assess user access privileges, including procedures for the approval of creation, modification and deletion of user access;**
- **Assessing, scanning, validating, prioritizing and remediating application and infrastructure security vulnerabilities;**
- **Use of advanced data loss prevention technologies and processes;**
- **Internal control testing of important aspects of security and technology solutions and processes across the technology systems and business;**
- **Monitoring and investigating potential or actual security events in accordance with Ambac's incident response plan;**
- **Providing secure solutions for the transmission of personal, confidential and proprietary information to third parties; and**
- **Overseeing the onboarding and management of third-party providers to ensure appropriate security controls are in place, and technologies offered by third party providers are implemented and maintained in a secure environment.**

Ambac remains committed in its ongoing efforts to continually strengthen its systems for protecting data, information and intellectual property, and our policies, processes and standards evolve accordingly to enhance the Program and data privacy. Ambac regularly reviews and updates its information security policies and standards, in accordance with applicable industry leading practices and regulatory requirements.

Employees are required to keep confidential all information about employees, policyholders, and claimants, among others, and access the information only for designated business purposes. Guidance for employees on the use of information technology is also provided in Ambac's Code of Business Conduct and Ethics.

**Ambac cybersecurity policies and processes address:**

- **Access Management**
- **Application and Device Management**
- **CCPA Compliance**
- **Cybersecurity**
- **Data Protection**
- **Disaster Recovery and Business Continuity**
- **Network Security**
- **Physical Security**
- **Risk Management**
- **Third-Party Risk Management**

**Several expanded highlights within our Information Security and Risk Mitigation Programs:**

## Information Security Risk Assessment

To protect our information and data, we utilize multiple layers of defense: individual employees across the enterprise, the information security program, and assessments. The information security program includes assessments with multiple layers of testing and measurement, as well as vulnerability assessments for known threats, and mandatory training sessions for all employees. The information security program incorporates tools and technologies to better find, categorize, prioritize and respond to vulnerabilities.

The company also subscribes to third party threat intelligence services to monitor dark web and internet threat activity to our data or sensitive information. We also track industry and government intelligence sources for impact in the marketplace and deploy necessary updates as appropriate. Additionally, new laws and regulations are monitored for potential impact to Ambac's operations, and we endeavor to revise our controls, as needed.

## Monitoring and Responding to Data Breaches

In addition, Ambac deploys tools and technologies to detect, prevent and mitigate threats and cyber-attacks. These tools, technologies, and processes are continually improved in an effort to reduce risk, decrease response time, and improve effectiveness of actions and identification of threats. Ambac has an incident response plan that provides a key framework for responding to cybersecurity incidents and data breaches. The company is committed to providing notices of a data breach in a timely manner to individuals and regulators, as required by law.

## Training on Information Security

Data and information security starts with our own people. In order to reduce risk and better prepare staff against online threats, all employees of Ambac and its subsidiaries, and consultants receive annual cybersecurity awareness training, which is reinforced with periodic phishing campaigns.