Gartner

Information Security at Gartner

Gartner

A message from our Executives

The confidentiality of our clients' information is extremely important to us. Our policies, systems and security controls are developed to protect our clients' information as well as Gartner's intellectual property.

We have a comprehensive Information Security Program to prevent unauthorized access to client information and to protect against known and evolving threats. We employ a defense-in-depth strategy, which means that multiple layers of security protect our data assets. These technology layers include firewalls, intrusion prevention systems, log monitoring, real time alerts, vulnerability scanners and anti-virus protection—to name a few.

Our technical security solutions are complemented by industry-standard policies and best practices. Need-to-know and principle-of-least-privilege practices are followed throughout the organization. We maintain multiple industry-standard certifications in diverse service areas. We are aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and certified to the International Organization for Standardization (ISO) standards for information security. Our Information Security Program is continually reviewed and validated by independent regulatory institutions and third-party security assessment organizations to ensure that we continue to meet or exceed security expectations.

We design our Information Security Program to be compliant with laws, regulations and best practice policies, while maintaining client information security as a top priority.

Thank you for your interest in the Information Security Program at Gartner. The security booklet that follows provides an overview of our program. Please note that all references to Gartner in the security booklet are intended to include Gartner, Inc. and all of its wholly-owned subsidiaries (collectively, "Gartner") as further described in the Introduction below. If you have any questions, do not hesitate to contact us or any member of the information security team.

Altaf Rupani
Executive Vice President & CIO
Direct: +1-203-340-0921
E-Mail: altaf.rupani@gartner.com

Zack Gillette
Chief Information Security Officer
Direct: +1-475-685-5847
E-Mail: zack.gillette@gartner.com

Table of Contents

Introduction

Gartner is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with the indispensable insights, advice and tools they need to achieve their mission-critical priorities and build the organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are trusted as an objective resource and critical partner by more than 12,000 organizations in more than 100 countries—across all major functions, in every industry and enterprise size.

This document, which is intended to cover Gartner, Inc. and all of its wholly-owned subsidiaries (collectively, “Gartner”), explains Gartner’s approach to information security and describes the processes and technologies used to protect information and information systems. It answers questions that our clients regularly ask to ensure their data is protected and to satisfy legal and regulatory requirements.

Gartner Takes Information Security Seriously

Gartner has a strong security culture. Its operations depend on complex, interconnected information systems and networks. To protect the confidentiality, integrity and availability of the data these systems and networks store, process or transmit, we use a layered or “defense-in-depth” strategy. We rely on technology and human processes to safeguard our client’s data at all layers. We embed appropriate controls within our business processes and technology development, starting with design and engineering and extending to operations.

Information Security Team

Gartner’s Information Security team consists of practice areas dedicated to delivering a comprehensive security strategy. Our team includes some of the foremost experts in application security, network security, and threat detection. Our team draws upon multiple disciplines in order to deliver proactive information security protection while preventing, detecting and responding to internal and external threats to Gartner. The Information Security team covers a wide range of security responsibilities, including security architecture, technology security assessment, application security, penetration testing, vulnerability management, security engineering, identity and access management, risk management, business continuity management, security monitoring, and incident response.

Data Protection Program

Gartner recognizes the importance of having effective and meaningful privacy protections to govern the collection, use, analysis, processing and disclosure of confidential information, including (but not limited to) personal information. Our data protection program is aligned with our obligations to our clients and our associates under all applicable data protection laws. All Gartner entities around the world operate the same level of technical, physical, and administrative security controls and are required to comply with our data protection policies, procedures and applicable laws.

We also have an Intra Group Data Processing Agreement in place (signed by all Gartner entities) containing the European Union ("EU") Standard Contractual Clauses, which have been approved by the EU data protection authorities for the transfer of data outside the European Economic Area.

When service providers or other third-party vendors are engaged to perform services on our behalf, we perform due diligence to ensure that those providers have appropriate privacy and security controls in place. We contractually require these providers to implement appropriate technical, security and privacy measures, and to only use confidential information solely for the purposes of performing their services.

Our Approach is More than Compliance

Cyber threats are evolving at an accelerated rate, and often robust compliance efforts are not enough to keep abreast and ahead of the ever-changing threat landscape. While adherence to laws and regulatory bodies is imperative, we combine a risk-centric, threat-informed strategy to best tailor our control solutions—while meeting or exceeding compliance requirements.

Strong Security Culture and Awareness Training

Gartner understands the importance of a strong security culture. We have an engaging and comprehensive security training and awareness program for all Gartner associates and third-party contractors. Associates receive security training upon arrival at Gartner, with awareness and training activities provided throughout their employment. During new hire onboarding, associates attest to our Code of Conduct and Acceptable Use Policy, both of which highlight our commitment to ethically protect our customer data. Our ongoing awareness and training program leverages a mixture of communications and simulated attacks, to include phishing, for reinforcement of good behaviors and to drive awareness of current attack techniques. Additionally, strong partnerships exist among Gartner business partners—including Legal, Compliance, Risk, Human Resources and our Technology teams.

External Stakeholders and Research Community

Our security program draws on Gartner's rigorous research and advisory methodologies to bolster our program's insights. To help strengthen our security program, we leverage our Gartner analysts' years of experience observing trends and best practice delivery of security technologies and processes. Gartner research is used to assist in evaluating and acquiring relevant information security tools and services. Externally, Gartner maintains active relationships with the local law enforcement agencies and the broader information security community.

Employee Background Checks

Where permitted by applicable local law, including employment and data protection laws, Gartner conducts reasonable pre-employment background checks on all associates joining the company. This may include reference checking, verification of prior education and employment, criminal background evaluation, credit reference and other security checks.

Independent Third-Party Compliance & Certifications

Gartner understands that the confidentiality, integrity, and availability of information we process is of paramount importance to our current and prospective clients. Furthermore, the intellectual property we hold and the software products we develop are essential to the future success and growth of our company. To ensure Gartner products and services are reliable, safe and of high quality, we undergo several independent third-party audits and reviews on a regular basis. As part of the audit and review process, independent auditors examine our data centers, infrastructure and operations to verify Gartner security, privacy and compliance controls. Our commitment to a secure operating environment is demonstrated by our ongoing certification program.

ISO 27001: Information Security

Gartner maintains certification with ISO 27001. We have developed and implemented a comprehensive Information Security Management System (ISMS). Gartner applies a systematic approach to securely managing sensitive, confidential information by implementing best-practice information security policies, systemized controls and risk management processes. We adopted an overarching management process to ensure that information security controls meet our information security needs on an ongoing basis.

SSAE 16/SOC 2 Type II

Gartner uses third-party co-location facilities to support technology services in an environment that provides flexibility, scalability, and security. Our U.S.-based co-location data

centers are SOC 2 Type II certified. The trust service principles on which SOC 2 is based are modeled on five principles: security, availability, processing integrity, confidentiality and privacy. Each of these principles have defined controls that must be met to demonstrate adherence to the principles and to produce an unqualified opinion during an independent audit.

National Institute of Standards and Technology (NIST) 800-171

Gartner understands the importance of protecting Controlled Unclassified Information (CUI). We have established uniform policies and practices to ensure alignment with NIST Special Publication 800-171. In addition to defining and implementing safeguard requirements for CUI, Gartner maintains an up-to-date System Security Plan (SSP) and Plan of Action and Milestones (POAM) to ensure compliance with NIST 800-171.

Sarbanes-Oxley (SOX)

As a publicly traded company, we have developed specific controls to protect our financial processes and reporting obligations. Our internal and external auditors perform an annual evaluation of SOX control effectiveness. This evaluation includes, but is not limited to, controls over Access Security, Change Management, Program Development and Computer Operations.

Payment Card Industry (PCI) Data Security Standard (DSS)

Gartner remains Payment Card Industry (PCI) compliant by ensuring adherence to PCI data security standards. We accept certain payments utilizing third-party companies who are PCI-certified. Gartner does not directly store, process or transmit cardholder data.

Governance and Risk Management

Gartner has a comprehensive, systematic governance and risk management process for managing risk. Our program provides ongoing risk oversight, risk management and control over material business risks. Our approach to risk management is to minimize the effects of compliance, financial, operational, reputational, and strategic risks, while accepting a reasonable degree of managed risk in pursuit of our mission and objectives.

Internal Audit

An independent Internal Audit function conducts routine audits across the enterprise to ensure controls are in place to protect Gartner and client assets. Internal audit co-sourcing is often utilized to ensure a breadth of experience and resources. Internal Audit activities

(including Risk Assessments) are regularly communicated to Executive Leadership as well as to the Board of Directors.

Information Security Risk Management

In addition to Risk Management at the enterprise level, the Information Security team has a dedicated Governance and Risk Management (GRM) program. This program identifies and assesses Gartner's business risks and partners with internal stakeholders to select the appropriate risk treatment plan. Risk management activities are regularly provided to the Board of Directors, Executive Leadership and Enterprise Risk Management.

Business Continuity Management

Gartner has a Business Continuity Management Program to prevent business disruptions in response to external and internal events. The process begins with a Business Impact Analysis (BIA) and risk assessment to identify risks and threats to the organization, its products and services, and key business functions. Based on this analysis, business continuity and disaster recovery strategies and plans are developed, recovery teams are identified and trained, and exercises are conducted to validate those plans and team capabilities.

Disaster Recovery

In the event of business disruption, Gartner has a disaster recovery capability to restore critical systems and applications in alignment with our business recovery objectives. Disaster Recovery Plans (DRP) provide documented step-by-step actions that must be taken to restore operations of systems or applications within established recovery time and recovery point objectives. Recovery teams are trained on roles and responsibilities to ensure consistent actions during and following a disruption.

Crisis Management

Gartner maintains a global crisis management program in alignment with industry best practices. The program includes a corporate crisis team. Regional crisis teams are in place in the Americas, EMEA, India and APAC. Training workshops and/or scenario-based tabletop exercises are conducted quarterly, capturing lessons learned following each session.

Enterprise Technology Security

Gartner utilizes multiple defense strategies in our approach to information security. These strategies ensure that numerous layers of security controls and mechanisms are in place throughout our IT ecosystem. Our IT Infrastructure services are aligned with industry best practice. Controls, processes and procedures are in place to protect the availability, integrity, and confidentiality of Gartner infrastructure.

Vulnerability Management

Gartner utilizes a vulnerability management process that leverages external vendor services, as well as a suite of security scanning and penetration testing tools to identify, validate, and prioritize vulnerabilities. A designated security team is responsible for tracking and ensuring vulnerability remediation. Once a vulnerability requiring remediation has been identified, it is logged and prioritized based on its severity, and an owner is assigned. The security team tracks such vulnerabilities until remediation is verified. We employ a monthly patch management process unless criticality dictates otherwise. Remediation of vulnerabilities is addressed directly within relevant application and infrastructure teams in accordance with policy and service level agreements.

Multi-Factor Authentication

Gartner employs Multi-Factor Authentication (MFA) as an additional layer of security to protect against threats. We utilize a two-factor solution that uses asymmetric cryptography. MFA is required for any remote access that is off the Gartner network, including access to cloud or web applications.

Identity Access Management

Identity and Access Management (IAM) is critically important at Gartner. We employ the principle of least privilege, and access is restricted to the minimum entitlements necessary for associates to perform their role. Our IAM function utilizes a robust framework of policies and technology solutions that are fully integrated with all relevant business processes. This framework allows for a centralized and consistent way to ensure associates have the appropriate access to technology and data resources.

Endpoint Security

Gartner utilizes a holistic approach to endpoint security to protect our data. All endpoints are protected with a Next-Generation Antivirus (NGAV) and Endpoint Detection and Response (EDR) technology which employs heuristic, behavior-based detection capabilities in conjunction with traditional signature-based detection. Additionally, Gartner's endpoint

solution provides host-based intrusion prevention (HIPS) to prevent exploitation. Application whitelisting and privileged access management is utilized to ensure the concept of least-privilege is enforced, allowing any potential compromise to remain at the user level and preventing lateral movement. Gartner proactively conducts threat hunting to identify suspicious activity. Our processes and technology enable us to quickly isolate an endpoint device in the event of a suspected compromise. We inspect and proxy all endpoint traffic to identify and block suspicious activity.

Mobile Security

Gartner understands the risks and concerns associated with the use of mobile technology. We develop policies and standards that define our approach for protecting mobile portable computing devices, and the networks they connect to. These security policies are reviewed and measured against industry standards to ensure the safety of client data. We use a secure industry best practice Mobile Device Management (MDM) solution to simplify and enhance the security and management of mobile devices. We restrict access to proprietary data from mobile devices by requiring enrollment in our MDM program. Our MDM solution enforces a set of security configurations and standards in alignment with our security policies.

Application Security

Gartner is committed to protecting the integrity of all data housed within its applications. Application security is validated by running static and dynamic application scanning tools, and conducting manual penetration testing to identify and remediate application code vulnerabilities before applications are moved to production. Application security assessment reviews are a crucial part of our software development lifecycle. Each application goes through a security review and assessment process where evidence of compliance with security controls are validated and tested. Assessment results are used to improve the overall security posture of application and platform products prior to release. The security of the application environment is monitored by regular scans to identify needed operating system, middleware and application patches.

Data Security

Gartner protects the security of client data both at rest and in transit. Data at rest is protected by employing persistent encryption where possible. In Gartner’s cloud environments, data at rest is encrypted by utilizing the native encryption services offered by the cloud provider. Where we have identified data that is very sensitive, additional symmetric or asymmetric encryption may be used on top of native encryption protocols. For databases, the persistent encryption options offered by the Database Management System (DBMS) vendor are used.

Data in transit is encrypted throughout its lifecycle of interaction. As data enters an application, accepted protocols such as Transport Layer Security (TLS) or Secure Shell (SSH) are used to ensure the data is protected in transit.

Network Security

Access to Gartner networks is tightly controlled. Perimeter firewalls are used at every ingress/egress point. Firewall rules prohibit external to internal access without prior authorization by Gartner Information Security. Security exceptions for business-to-business communications require appropriate authentication, encryption and network protocol filtering based on least privileged principles. External user access to Gartner is controlled via Virtual Private Network (VPN) and TLS for web portal access. All non-employee access includes automatic expiration dates. Wi-Fi access and VPN access require passwords and appropriate second factor authentication mechanisms. Wi-Fi systems use Wi-Fi Protected Access (WPA)-2 with Extensible Authentication Protocol (EAP) extensions for authentication. Network based spam filtering is used to reduce the risk of spam becoming a vector for malware attacks.

Web Security

Gartner uses a ‘best-in-class’ global cloud-based security gateway service to improve our overall Internet and Web security. We utilize malware detection, content filtering and inspection capabilities across all endpoints, regardless of location. Our processes and technology enable us to deliver enhanced security, better visibility to threats, enforcement of HR policy and a secure Internet experience.

Event Monitoring and Logging

Gartner uses an industry-leading Security Information & Event Management (SIEM) system coupled with a Security Orchestration, Automation, and Response (SOAR) process and platform for event monitoring, log aggregation, and real-time response. Expanded coverage of log sources integrated with the SIEM solution increases our ability to detect malicious activity within our technology environment. Behavior analytics and insider threat indicators complement our capabilities to identify anomalous behavior to protect against insider threats. Our SIEM data is enriched by multiple external threat intelligence feeds and other data to provide additional indicators of compromise.

Incident Response

Gartner utilizes a documented incident response process. In the event of a suspected or confirmed incident, the Information Security Team coordinates incident response activities with representatives from each IT discipline, as well as from Physical Security, Legal and

Corporate Communications. Our Incident Response team leverages a suite of tools and best practices to efficiently and effectively manage an incident throughout the incident response lifecycle (Detection, Analysis, Containment, Eradication and Recovery).

Product Security

Gartner's security teams perform numerous activities to ensure that our products are secure. We have various policies, procedures and programs that enable our product teams to deliver solutions that are best in class when it comes to security and compliance with laws and regulations.

Secure Development

Associates with development responsibilities are required to undergo Secure Development training. Applications are developed following a defined software development lifecycle process, which ensures products are secure during design, while in development and after they have been deployed. Development and testing take place in a separate environment from production.

Application Testing

Application security testing is a critical security activity embedded into the software development life cycle to reduce the risk of vulnerable applications and associated business risk. Application code is tested for vulnerabilities using software composition analysis, static and dynamic code scans. Internally and externally managed penetration tests are conducted to identify application-level vulnerabilities. Identified vulnerabilities are remediated by members of the application and security teams.

Change Management

Gartner has a formal change management process where changes are reviewed by a Change Advisory Board (CAB). Changes are reviewed and tested after moving into a staging environment, then additional testing is performed by IT and the business application owners prior to deployment into Production. Backout plans are required to minimize service disruption.

Physical Security

The safety and security of Gartner associates and assets is a priority. Gartner uses a combination of owned and leased office space. We employ and support a layered security model. Our sites are protected by a combination of access controls, intrusion detection systems, visitor management as well as video surveillance.

Gartner Facility Access and Personnel Access Control

Security and safety designs are constructed to protect people and infrastructure in alignment with risk and in partnership with our real estate providers. Physical security and safety designs are constructed to protect people and infrastructure in alignment with risk. All associates and approved third party individuals are required to use the Gartner access control system for accessing Gartner facilities. In addition, some associates will be issued keys/credentials to access specific areas within an office.

Data Center Security

Gartner's data center providers utilize physical security boundaries and entry controls to prevent unauthorized physical access, damage and interference to information processing facilities hosting Gartner data.

Security Guards Security

Security guards are present at many of our sites for building security. We have a dedicated guard force at primary campuses and facility-provided security at most other sites.

To learn more, contact your Gartner representative.