Technical and Organizational Measures

Cloud Based Applications for the Management of Lockers and Access Control Devices

1 SCOPE

The technical and organizational measures described below apply to GANTNER's cloud solutions for the management of lockers and access control devices that are referred to these technical and organizational measures in its applicable data processing agreement.

GANTNER reserves the right to modify and update these measures at any time without notice as long as we maintain a comparable or better level of security.

2 LIST OF TECHNICAL AND ORGANIZATIONAL MEASURES

Below you can find the list of security measures applied by GANTNER:

> **Security Policies:** GANTNER implements security policies and standards that are mandatory across the organization. Security policies are reviewed periodically and updated if needed to mitigate the risk exposition and maintain platforms and data secure.

> **Security Awareness:** GANTNER conducts regular awareness campaigns across the organization to prevent and mitigate users' risks.

> **Physical Security:** GANTNER protects its facilities using appropriate access control systems (e.g., smart door locks) to restrict access to authorized personnel. In addition, secure areas such as data centers have additional protection measures against environmental threats. To protect proper functionality, protection measures (air conditioning, fire extinction etc.) undergo maintenance on a regular basis. In addition, GANTNER uses trusted third party colocation providers which also incorporate physical security controls in compliance with industry standards.

> **Security Incidents:** GANTNER maintains incident response plans including personal data breach management.

> **Access Control:** GANTNER implements appropriate access control to ensure access to the applications and systems in general is restricted according to least privilege and need to know principles. All personnel access GANTNER's systems with a unique identifier (user ID). In case personnel leaves the company, their access rights are revoked.

> **Network Security:** GANTNER employs encrypted and authenticated connections for connecting to platforms and systems in general by using security capabilities such as firewalls, VPNs, authentication mechanisms, etc.

> **Secure workstations:** GANTNER implements appropriate protection over end user's devices such as advanced antimalware protection, hard disk encryption and appropriate patch levels.

> **Privacy and Security by design:** GANTNER applies privacy and security by design principles when adopting a new system or enhancing an existing one.

> **Vulnerability Management:** GANTNER conducts security reviews on a periodic basis and remediate the identified vulnerabilities in order to maintain platforms secure.

> **Resiliency:** GANTNER adopts backup and disaster recovery plans for adverse situations.

> **Assurance:** GANTNER conducts regular reviews to ensure compliance with the security policies and standards.

Last update: February 2026