

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Description of the technical and organisational security measures implemented by GTT for each Service provided.

1 PHYSICAL

1.1 PHYSICAL SECURITY

GTT shall implement:

1.1.1 a building access control system for the Site;

1.1.2 appropriate CCTV for the Site.

1.2 EMPLOYEE, VISITOR, AND TRUSTED AGENT ACCESS

In areas where Services are being provided, GTT shall:

1.2.1 restrict access to authorized persons only;

1.2.2 utilize identification and authentication controls to authorize and validate the access;

1.2.3 securely maintain an audit trail of all access, including times of entry and departure;

1.2.4 securely manage visitors:

(a) grant access only for specific authorized purposes;

(b) record the date and time of entry; and

(c) ensure that all visitors are escorted and supervised at all times.

2 TECHNICAL

2.1 SYSTEM ADMINISTRATION

2.1.1 Where systems allow, all privileged accounts shall be uniquely identifiable and each user shall be accountable and responsible for any action taken under that user's own user ID and password.

2.1.2 Where systems allow, system accounts or built-in application accounts shall not be used or renamed.

2.1.3 All access to Information Systems shall be authenticated. This includes console access, individual accounts, administrative accounts, and any automated relationships with other systems.

2.1.4 GTT maintains an MDM policy, with all laptops being encrypted. USB ports have been disabled, and a VPN solution is in place.

2.2 PASSWORD CONTROLS

2.2.1 Passwords shall be protected at all times, including appropriate encryption.

2.2.2 All passwords shall be promptly changed if they are suspected of being compromised or known to have been disclosed to unauthorized parties; users shall be able to change their own passwords.

2.2.3 Where systems allow, passwords shall be uniquely identifiable and each user shall be accountable and responsible for any action taken under that user's own user ID and password. Users shall not share or divulge their password to anyone.

2.2.4 On rare occasions where the requirement of hardcoded usernames and passwords is necessary and where systems allow, the system will be configured with a service account with the lowest set of privileges possible.

2.2.5 Where systems allow, passwords complexity should never be less than 3 out of 4 character classes and shall have character class choices such as upper case letters, lower case letters, numeric digits, or special characters. Where possible an increased password length will be used to increase entropy probabilities.

2.3 SEGREGATION CONTROL

Where the customer solution utilises a shared environment, appropriate security controls will be deployed to ensure appropriate customer segregation.

2.4 PERIMETER DEFENCE

Firewalls and intrusion detection systems are placed to monitor and resist malicious activity.

2.5 OPERATING SYSTEM SECURITY CONTROLS

2.5.1 Anti-Virus Configuration

Anti-Virus software can be supplied as a service and configured upon the Customers express consent. Where this service is provided it will be configured to run real-time and to download automatic updates no less than once per week.

2.5.2 Patch Management

Where possible patch management systems are in place to deploy critical security patches to GTT managed devices. For customer facing services, patches will not be deployed without a customer request to do so.

2.6 SYSTEM AND DEVICE HARDENING

Where possible all operating systems and devices will be hardened to remove any weak protocols and services that are not required.

2.7 VULNERABILITY DISCOVERY

Where possible regular system vulnerability scanning will be carried out with the express permission of the customer to identify any technical issues that may need to be resolved.

2.8 EMAIL SECURITY

GTT employs a multi-layered approach to safeguard its email ecosystem against malicious threats. In addition to traditional email security gateways, the company has deployed an advanced AI-powered tool to detect and mitigate sophisticated phishing attempts and malware attacks.

GTT has implemented Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols to combat email spoofing and enhance email authentication mechanisms.

3 PROCESS

3.1 SYSTEM ADMINISTRATION

3.1.1 Privileged account requests shall be subject to proper justification, provisioning and an approvals process, and assigned to named individuals

3.1.2 GTT Service Provider personnel privileges shall be reviewed to ensure they have the appropriate privileges to undertake their duties

3.1.3 Starters and leavers process is in place to remove accounts that are no longer required.

3.2 INFORMATION SECURITY AND DATA PRIVACY TRAININGS

3.2.1 Staff information security and data privacy trainings are performed at least on annual basis. Regular information security communications are provided to all staff. Information security policies are available to all GTT employees and are mentioned throughout the information security awareness training lessons. A set of policies are formally acknowledged via Workday.

3.3 ACCESS CONTROLS TO DATA

The GTT Service Provider shall follow Customer instructions with regards to the movement of data. All requests to move customer data shall be made in writing to the GTT Service Provider.

3.4 DESTRUCTION OF MEDIA

All hard drives shall follow GTT's processes and procedures for their erasure or destruction prior to disposal of the system.

3.5 DISCLOSURE CONTROL

The GTT Service Provider shall not:

3.5.1 allow copying of customer hosting environments other than for back up or forensic purposes; and

3.5.2 allow the removal of Customer Personal data from the premises unless at the specific request of the customer.

3.6 SUPPLIER MANAGEMENT

Any suppliers or contractors with direct access to platform, or system data must have appropriate contractual obligations applied to maintain the confidentiality of data and comply with applicable GTT security policy controls.

GTT shall use reasonable endeavours to impose obligations in relation to the Processing of the Customer Personal Data that are equivalent to those imposed on GTT.

The subcontracted service provider shall employ appropriate operational and technological processes and procedures to keep Personal Data safe from unauthorised access, loss, destruction, theft or disclosure.

Third party risk management program has been implemented, aimed at evaluating GTT's vendors and risk scoring them.

4 CUSTOMER RESPONSIBILITIES IN RELATION TO DATA CONFIDENTIALITY AND ENCRYPTION

- 4.1 GTT recommends that the Customer further protects the confidentiality of the Customer's data with additional cryptographic controls. Such controls would include encrypting data at rest through application and database level encryption. In addition, the application controls should ensure that all access to sensitive data is tightly controlled through strong access control mechanisms and all such access is thoroughly audited.
- 4.2. It is customer's responsibility to manage the cryptographic keys used for the protection of data by the customer. The customer's key management system should be designed with consideration of the same concerns about protecting data at rest.