Information Security Policy and Information Management System for Testimonial Tree

Revised June 2021

Introduction

Testimonial Tree is designed and managed with the highest level of security and integrity in mind. Testimonial Tree has developed its own compliancy regime as further set out in this Information Security Policy (ISP). TT's Services have been designed to implement the security requirements to systematically and safely protect customer data as an International Organization for Standardization (ISO) Information Security Management System (ISMS) based on ISO 27001:2013 and other ancillary ISO standards.Testimonial Tree considers information security to be a high priority and has established company-wide policies to ensure all personnel understand their responsibilities in the protection of information in order to maintain data confidentiality, integrity, accessibility, availability, and privacy. Testimonial Tree provides its employees with communication systems, hardware, and software necessary to conduct business. All Testimonial Tree employees must comply with Testimonial Tree security policies and procedures when utilizing company information technology assets. Testimonial Tree employees that are a part of the Testimonial Tree are trained on Testimonial Tree security policies and are expected to apply and extend those concepts to fit the needs of day-to-day operations.This document applies to all employees, contractors (to include consultants and temporary staff), and other employees of theTT Operations team.

Purpose

This Information Security Policy (ISP) provides a commitment to establish:
(i)procedural requirements and technical guidance to manage information security.
(ii) those processes and resources necessary for the business unit to secure company information from threats against proprietary intellectual property rights, sensitive customer or partner data under our control as well as data with privacy requirements.
(iii)general business productivity, in recognition of the vital role that information plays in the managing of risks to the Customer’s business.

Scope

The general objective of the Information Security Policy is: the establishment, recording and communication of objectives, key points and preconditions of Testimonial Tree Operations with regard to the security of the information provision of TT’s Services. Information security is based on three quality aspects:

1) Confidentiality
2) Integrity
3) Availability.

Confidentiality

Guaranteeing the confidentiality of information comprises measures that ensure:
-Exclusivity of information: programs, data and equipment are only accessible for those who have explicitly been authorized for this.
-Protection of privacy when storing and using information.

Integrity

Guaranteeing the integrity of information comprises measures that, with regard to data, software and information distribution, ensure:
-Accuracy and consistency.
-Validity.
-Completeness.
-Verifiability.
-Authenticity.

Availability

Guaranteeing the availability of information comprises measures that ensure:
-Continuity.
-Timeliness.

Roles and Responsibilities

The ISMS for Testimonial Tree is operated and maintained by the following groups: Testimonial Tree IT, Compliance Manager, Human Resources (HR), and the Chief Executive officer (CEO), and the Corporate Executive board.

The Board is responsible for all executive decisions as the approving body of all financial and major strategic decisions for the TT Operations business unit. The following are additional responsibilities of the CEO and the Board:
-Providing the strategy objectives on corporate level.
-Review and recommend decisions to the TT Management(specified above).
-Approve significant investment requests.

Information Technology Department
The IT Department (IT) is responsible for providing corporate level IT support. IT also manages the assets with coordination of the TT Management and all user access and account management duties with respect to Testimonial Tree employees. Specific roles and responsibilities of the Testimonial Tree ISMS is handled by the business unit.

Human Resources
The Human Resources department(HR)is responsible for handling the management of all Testimonial Tree personnel and Testimonial Tree personnel data as it relates to their employment with TT. HR is responsible for the investigation and vetting of all Testimonial Tree employees, contractors and vendors. HR is responsible for communicating new hires to the CEO to each of TT's business unit's management personnel and to ensure that users access is coordinated by the IT Department and/or business units. Any non-compliance with Testimonial Tree policies will be reported to the appropriate employees' management and handled by the HR department accordingly.

Testimonial Tree Team Management

The Management of the Testimonial Tree includes the CEO of TT and Team Leaders of the TT Team. These personnel are responsible:

-for taking part in regularly scheduled and ad hoc management review meetings.

-the overall accountability of the information security, governance, and compliance of the Testimonial Tree ISMS.

-Allocating adequate resources for managing the information security.

-Allocating ownership to information and information systems.

-Ensuring adequate knowledge and awareness with regard to information security among employees and contractors.

-Guaranteeing that the roles, tasks and responsibilities are recorded in the job descriptions of the employees and in contracts with third parties(including contractors).

-Periodic monitoring as to whether employees and contractors comply with the Information Security Policy and related regulations and procedures.

-Taking necessary security-related measures following alterations of tasks and responsibilities of employees, suspension or termination of employment, termination of assignments or contracts.

-Communicating, within their own area of responsibility, the necessity of information security and the applicable policy regulations (awareness);

-Offering support with the implementation of the organization-wide common reliability standards and security measures and monitoring this; and

-Establishing operational guidelines and procedures in relation to information security (tactical/operational).

Customer Service Manager

The Service Manager of the Testimonial Tree business unit is responsible for managing the service and governance of service delivery processes. Their main responsibilities are to ensure that service level objectives are met and that service delivery processes are followed.

The following are additional responsibilities of the Service Manager:

-Implementing and managing theIT Infrastructure Library(ITIL) based processes of Incident, problem and change management;

-Measuring service levels and assuring that they are on appropriate levels;

-Chairing the change approval board meeting;

-Making sure that service delivery processes are delivered in line with security and compliance requirements.

-Managing communication with customers.

Compliance Manager

The Compliance Manager of Testimonial Tree Operations is responsible for the overall compliance and governance of the TT's ISMS with the direction of the Head of TT Operations and the CEO.

The following are additional responsibilities of the Compliance Manager:

•Develops operational strategies for compliance with data protection legislation;

•Ensures that the policy and standards for compliance with data protection legislation are fit for purpose, current and correctly implemented;
•Accountable for embedding security within theTTTT Operations business unit by identifying security threats and risks, and enabling project teams to develop and deliver control strategies;
•Engages with the stakeholders for change programs to ensure adequate security safeguards are being managed to monitor security risks and threats;
•Delivery of mitigation strategies for identified weakness, vulnerabilities and security threats; and
•Reviews new business proposals and provides specialist advice on compliance issues
•Responsible for the preparation for security and compliance audits held by customers or third-party certification organizations.

The TT Engineers are members of the Testimonial Tree Operations team that are responsible for the day-to-day execution of their duties to maintain and monitor the Testimonial Tree ISMS.
The following are additional responsibilities of TT Engineers:
-Follow the information security policies and procedures
-Adhere to security best practices
-Proactively identify any security risks or incidents within the organization
-Provide technical support with solving security incidents.

Segregation of Duties

Testimonial Tree Operations will segregate conflicting duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.Testimonial Tree Operations will identify each major role and briefly describe the duties to ensure the correct actor has the properly allocated responsibilities. For example, these might be Testimonial Tree ISMS system administrators, corporate system administrators, and customer application administrators. Each role will have separately defined duties.

Testimonial Tree Operations will address each management role separately to ensure that only authorized persons can approve changes to the systems. This can also ensure such things as ensuring that financial control is not inadvertently given to someone who will only have basic user access. For example, a developer should not also act as security manager, likewise, clerical staff should not act as a finance officer.

Compliance Requirements

This section describes the requirements of International Organization for Standardization/International Electrotechnical Commission that are addressed within this document:

Information Security Policies

Management direction for information security: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

-Policies for information security: A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
-Review of the policies for information security: The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Organization of Information Security

Internal organization: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

-Information security roles and responsibilities: All information security responsibilities shall be defined and allocated.

-Segregation of duties: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
-Contact with authorities: Appropriate contacts with relevant authorities shall be maintained.
-Contact with special interest groups: Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
-Information security in project management: Information security shall be addressed in project management, regardless of the type of the project.

Mobile devices and teleworking

To ensure the security of teleworking and use of mobile devices.

-Mobile device policy: A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

-Teleworking: A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Compliance

-Compliance with legal and contractual requirements: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

-Identification of applicable legislation and contractual requirements: All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

-Intellectual property rights: Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

-Protection of records: Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

-Privacy and protection of personally identifiable information: Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
-Regulation of cryptographic controls: Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

-Information security reviews: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Independent review of information security:

-The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

-Compliance with security policies and standards: Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

-Technical compliance review: Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.

Testimonial Tree policy that addresses information security for all personnel.

-Establish, publish, maintain, disseminate, and have employees confirm by signature the security policy.

-Review the security policy at least annually and update the policy when the environment changes.

-Develop usage policies for critical technologies and define proper use of these technologies.

-Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

-Assign to an individual or team the information security management responsibilities outlined below.

-Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.

-Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks

include previous employment history, criminal record, credit history, and reference checks.)
-Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data.

Information Security Policy

Information Security Objectives and Planning

Testimonial Tree Operations has established information security objectives consistent with this ISP, which establishes procedural requirements and technical guidance to manage theTestimonial Tree ISMS.

The goals of theTestimonial Tree ISMS are as follows:

-Establish and maintain Testimonial TreeTTOperations roles and responsibilities for information security.
-Protect company data while making it available when needed to authorized entities for authorized use.
-Manage external and internal threats by implementing controls on data and devices.

Testimonial Tree Operations pursues four overriding goals for the information security and has implemented and documented the information security controls to:
-Preserve confidentiality, integrity, accessibility, availability, and privacy of information assets.
-Fulfill the requirements of this ISP.
-Achieve the information security management goals.
-Manage risks related to the information security.

Testimonial Tree Operations has created information security metrics that have been defined to align with information security objectives and are documented in the organizational metrics table. These measures are monitored, analyzed, and reported via the monthly metrics report in the executive reporting meeting. See the organizational metric table for additional information.

Testimonial Tree Operations employees will ensure information security is maintained, as follows:
-TT Operations will supply the processes, resources, training, and tools for a complete information security program.
-Data owners must establish and maintain sufficient preventive and detective security measures to ensure that the information for which they are responsible is fully protected.
-Managers must ensure that information security within their departments is treated as a regular business problem to be faced and solved, and must allocate sufficient resources and staff attention to adequately address information systems security and privacy.

Information security risks are defined as technical threats from external and internal sources, regulatory risks from failure to comply with laws and information security regulations for each country, region, or industry related to the business unit, risks to the loss of intellectual property or proprietary information, and mishandling of customer or partner data under contract and/or non-disclosure.
-All information systems security risks are tracked by the IT department and cataloged and quantified based on probability of occurrence and business impact. Controls are applied to

bring risks down to an acceptable level. Criteria for risk acceptability are as described in the Testimonial Tree ISMS Manual. Information security risks are continually monitored and adjusted through open sources, and internal tracking of threats to our infrastructure, industry, and the IT community.

See Appendix A: Ten Golden Rules for Information Security for best security practices that are employed within TT.

Approach to Information Security Information

As security is a continual process, reliable information provision demands continual attention. Alterations in the organization and/or the information provision, and the way in which the information provision is deployed for the purpose of operational management and process control, directly affect the reliability requirements demanded of the information provision and the measures that should be taken to ensure that.

Drawing up and implementing Information Security Policy

In this step, the objectives, preconditions and key points are recorded as well as the way in which the policy is translated into concrete measures. The policy is drawn up by the Compliance Manager.

Additional security

There are systems that demand higher reliability requirements (in terms of availability, integrity and confidentiality). The process of considering additional measures should be clear and reproducible, determined by the Compliance Manager and the CEO. The additional measures are subsequently implemented and communicated.

Security management and review

Information security requires a continual effort (security management) and is therefore not a one-off activity. Reliable information provision demands constant attention. Following implementation, it is checked that the measures are indeed executed as intended (review). Periodic evaluation is necessary to determine if the chosen measures still suffice and will be adjusted where necessary.

Under responsibility of the Compliance Manager, within the various business units, checks will be carried out on:
-The presence of adequate security plans.
-The compliance with the specified standards and the implementation of the necessary additional security measures.
-The involvement and care of management for the lasting effect of the measures.
In addition, investigations are carried out in the internal audits into the various aspects in relation to information security. The shortcomings, identified during the review, will be signaled and advice will be given regarding the measures to be taken in order to eliminate the faults

Management and Storage of Security Policies and Procedures

Testimonial Tree maintains all security policies within internal electronic document storage platforms.

Contact with Authorities and Special Interest Groups Authorities

Testimonial Tree maintains contact with all applicable authorities and other business units when necessary. Local authorities are notified and appropriate measures are coordinated with the police and fire department(s)in the event assistance is required.

Special Interest Groups

The Testimonial TreeCompliance Manager, who also acts as the Information System Security Officer (ISSO), attends conferences, training, and other events in order to stay updated with the current events of cyber security, governance, risk, compliance, and any other relevant information technology security topics and events.

Project Management

Information Security in Project Management

Information security is for Testimonial Tree, not an objective or policy per se, but an integral part of the business objectives and the management system of the operations. Correct security contributes to the business goals and to the reliable execution of the business processes. The aim is optimum information security throughout the project management lifecycle. Testimonial Tree Operations includes IT security risks in the risk management process. Testimonial Tree Operations ensures that risks are also evaluated by IT security persons to identify any related concerns. Testimonial Tree Operations will determine if there are IT security tests, reviews, or evaluations that would adversely impact the resources, schedules, or costs.

Project Management Process

The following describes the Testimonial Tree project management process.

Project Initiation

The project initiation phase consists of those processes performed to define a new project or a new phase of an existing project by obtaining authorization to start the project or phase. The initiation phase begins with defining the scope and initial financial resources for the project. The initiation phase also involves coordination with internal and external stakeholders.

Project Planning

The planning process establishes the total scope of the project and defines the objectives. The project management plan that emerges should clearly articulate the scope, time, cost, quality, communications, human resources, risks, procurements, and stakeholder engagement that the project requires to succeed.

Reliability Requirement

The basis of the information security is formed by the set of standards ('what'). These standards are subsequently translated, by the sections of the organization, into suitable, specific measures (‘how’). Every section of the organization is thus obliged to explicitly make a motivated statement about the desired security level and, by itself, identify measures based on classification and risk analysis. Every section of the organization should thereby, for its separate information systems, continually consider if the general level of security is appropriate, or if additional measures are necessary.

Project Execution

Executing the project can only begin once proper planning is complete. These are the processes in place to complete the work that has been outlined within the project plan to satisfy all the requirements.

Project Monitoring

The monitoring phase consists of the procedures used to track, review, and compose the progress of the project. Project monitoring consists of:

-Controlling changes and recommending corrective actions to risks/issues.
-Monitoring the ongoing project activities against the project management plan and performance metrics.

Risk analysis

Testimonial Tree perform cyclic risk analysis, whereby the threats to, effects on and vulnerability of the information systems and data, as well as the likelihood of these threats occurring, will be judged. Based on risk analysis, security

measures are determined whereby a security level acceptable to Testimonial Tree is realized. In determining the measures, the costs and benefits of these measures are considered. With regard to performing risk analysis, Testimonial Tree uses the following key points:
-The business units perform their own risk analysis.
-with the introduction of new information systems or important alterations.
-following an extensive security incident.
-at least once every three years for all company assets deployed for the most important business processes.
-The information resources and the implemented security measures are established and recorded.
-The risks are identified and the risk management strategy is recorded, for example:
-avoiding risks
-limiting risks
-allocating risks in third parties
-accepting risks

Risks that can lead to a considerable financial loss, damage or other negative consequences for Testimonial Tree are not accepted without explicit agreement of the responsible management.
-Risks accepted by the responsible management are reported to the Compliance Manager.
-The process for performing risk analysis and the results of the risk analysis should be documented and approved by the responsible management for the business unit concerned.
-The results of the risk analysis, approved by the responsible management, are reported to the Compliance Manager.

Project Closing

The project closing phase consists of activities performed to conclude all activities of the project lifecycle. This phase formally completes the project and all contract obligations for the Project.

Incident Handling

If TT becomes aware of any unlawful access to their TT Services, or unauthorized access to these services, or unlawful access to any Customer Data stored on AWS equipment or in AWS's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a 'security incident'), TT will promptly:

1. Notify Customer of the security incident.
2. Investigate the security incident and provide Customer with detailed information about the security incident.
3. Take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.

In order to be able to react appropriately to security incidents that may occur, these incidents will be classified. After a security incident is resolved, an evaluation takes place, and possible measures will be taken to prevent comparable incidents in the future or to limit the consequences of an incident.

Reporting and notifying Users who notice a (suspicion of an) incident or violation of the information security will report this to the Compliance Manager. Compliance Manager will take care of classifying the incident and of further settlement. Depending on the classification, the Compliance Manager will notify management and the applicable business unit’s.

Incident Priority and Severity Levels

The priority classification level list below provides several incident characteristics to assist proper incident classification. Moreover, if an incident contains characteristics in several different priority columns, the priority of an incident must reflect the most severe rating possible. Based on the incident urgency and impact, the incident priority matrix assists in determining the end priority.

Incident Urgency Category Description

High (H)

•Confirmed case of unauthorized access or modification of data.
•Reasonable suspicion that unauthorized access or modification of data happened.
•Actual theft of data.
•Identified unauthorized access to system.

Medium (M)

•Possibility of unauthorized access or data modification was identified, but there is lack of evidence of such happening
•Security patches not installed in timely manner.•Identification of gaps in firewall ruleset.
•Critical vulnerability found during quarterly vulnerability scan.

Low (L)

- Possibility of unauthorized access or data modification was identified, but there is lack of evidence that such vulnerability is exploitable as there are compensating controls in place.
- SQL injection vulnerability found in application, but mitigated by a Web Application Firewall(WAF).
- Not up to date antivirus definitions on host system with active network antivirus.

Incident Impact Category Description

High (H)

- Loss of confidentiality, integrity or availability of data classified as confidential
- Confirmed/Observation of ongoing organized targeted hostile action with the risk of theft or manipulation of confidential data or if a large amount of data is at risk.
- Theft of personally identifiable information(PII) from application.
- Unauthorized manipulation of financial data in the database.
- Identified advanced persistent threat.

Medium (M)

- Loss of confidentiality, integrity or availability of data classified as internal/proprietary
- Observations of preparations for organized targeted hostile action and high probability of loss or unavailability if countermeasures are not immediately initiated.
- Virus infection of an internal tooling server.
- Notification from a 3rdparty about a potential hostile action against IT environment (threat intelligence).

Low (L)
•Loss of integrity or availability of data classified as public.
•Defacing a publicly accessible website.
•Denial of service (DoS) attack on website containing only publicly available data.

Mobile Device Policy

TT does not allow employees to bring their own devices to work on the internal network. Employees are given a TT laptop and mobile phone for performing work on the TT Services ISMS. Users that are authorized to use personal mobile devices to access TT by using the organization's mobile app with the following security controls enabled on the devices:
•Minimum 4 character or biometric passwords must be enabled.
•Session lock after 15 minutes of inactivity.
•Automatic application wipe after 10 failed login attempts.
Users may use personal devices for incidental remote access purposes when authorized by business management. Note: in such cases, the user must be willing to surrender the device for inspection as requested by the IT Team unless doing so would be illegal under applicable local laws and regulations.

Users must NOT:
•Store or save organization confidential information on a personal device in any format (backup, attachment, etc.). Note: This does not apply to information stored in the organization mobile application.
•Connect personal devices to the TT internal network.
•Jailbreak, root or disable security controls in authorized personal mobile devices.

Unattended User Equipment Policy

Compliance Requirements

-ISO A.11.2 Equipment: To prevent loss, damage, theft, or compromise of assets and interruption to the organization's operations.
-ISO.A.11.2.8 Unattended user equipment: Users shall ensure that unattended equipment has appropriate protection.
-ISO.A.11.2.9 Clear desk and clear screen policy: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Unattended User Equipment

User equipment that is unattended must be locked prior to leaving the area of the equipment.

Clear Desk Policy

TT Operations does not authorize the use of removable storage media such as USBs, CDs, etc.

Compliance

Within TT Operations, the ISO27001 (Code of Practice for Information Security) is determined as the standard in which the guidelines to be used for information security are recorded. The demands of information security are recorded in the standards framework and are specified for each section of the organization. The intended measures all agree with these demands. In addition, TT Operations ensures that all policies and procedures have been finalized and approved by management. All TT Operations policies and procedures are reviewed and approved on annual basis or as significant changes occur.

Internal Audits

Internal auditors test, on behalf of management and in consultation with the Compliance Manager, whether the responsible line management of the business units realizes the policy and complies with the security standards. Reports of the internal audits go to management.

Standards

The TT compliance program gives customers confidence that the highest levels of security and data protection practices will be met and allows customers to streamline their own compliance with regulatory and industry standards.

•SOC 1–Report for service organization which are relevant to user entities' internal control over financial reporting.

•SOC 2–Report for service organization with controls for Trust Services Principles, which are security, availability, processing integrity, confidentiality and privacy.

•ISO 27001:2013–Provides requirements for establishing, implementing, maintaining and continuously improving the ISMS.
•ISO 27017:2015–An information security management system guideline dedicated to Cloud computing.

Security controls

Physical Security

TT Operations rely on data centers that feature state of the art facilities. These facilities include, at minimum, the following characteristics to ensure the highest level of security for customer data and platform infrastructure.

Data center Security -Asset Management
Data center has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide the services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets.
Data center Security -Controlled Access Points
Data center is located in a building that is physically constructed, managed, and monitored 24-hours a day to protect data and services from unauthorized access as well as environmental threats. CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.

Data center Security -User Access
Access to buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into data centers. Front desk personnel are required to positively identify

employees or authorized contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. Guests must be escorted by authorized TT personnel.

Data center Security -Unauthorized Persons
Entry Employees and contractors must have a business need to enter the data center and have received prior approval. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis.

Data center Security -Secure Area Authorization
Data center entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.

Network, Database and Application Security

Network level security features, process and protocols
•Secure access points and transmission protection –all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
•System security –Logical authentication and authorization mechanism in place.
•Firewalls –Stateful firewall technology to ensure only legitimate data enters the service environment.

Database level security features, process and protocols
•Data security –Logical authentication and authorization mechanism in place.

•Database security –Every customer has their own secure database which means partitioning of databases is not required and customer data is not co-mingled. The outcome is that a customer's data is never inadvertently shared with others.
•Databases (if option was ordered)and backups are encrypted using whole database encryption technology such as Transparent Database Encryption.

Application level security features, process and protocols
•Application access only –TT software architecture consists of separate and distinct user interface (screen), business logic and database tiers. This separation means that access to the user interface tier is distinct and does not provide direct access to the underlying business logic and database tiers.
•User/Role level permissions –TT applications allow for advanced granular permissions (Read, Write, Update, Delete) defined either by user or role and fully managed by the customer without TT involvement.
•Data level permissions –within a defined set of user/role permissions, TT applications allow for granular filtering of data, such as restrictions of which Customers a user is able to view or post invoices against.

•Idle disconnect –sessions are automatically logged out after a certain period of inactivity in order to protect accounts if users inadvertently forget to log out. Antivirus and Malware Protection Malicious software (malware, viruses, ransom ware, etc.) is a serious threat for IT infrastructures. The impact of malicious software can have far-reaching consequences for the continuity of TT's services. This plan describes the actions that are taken in the event that malicious software is detected in TT's service. All systems have antivirus software installed and are monitored to ensure the software is up to date as part of daily recurring preventive maintenance tasks.

Preventive measures:
1)Double-check that all antivirus software is up-to-date.
2)Check whether supplier provides separate preventive tooling.
3)Start preventive scan for other Customers.

Active measures:
1)Determine the source of the virus.
2)Repair damage:
a.Business critical aspects first.
b.Isolate contaminated systems or connections (switch off everything that is suspect).
c.Clean systems using software or tools.
d.If restore: place in quarantine location first in order to establish whether there is any contamination in the backup.
3)Update problem analysis with actions taken.

Security Testing

Periodic vulnerability and security tests take place to validate the security of TT. Both vulnerability and security tests are performed by a selected third party. Penetration tests include:
•Authentication
•Authorization
•Session management
•Info disclosure•Injections and input validation
•Encryption
•3rd party software.

TT does not externally release audit reports and results of security tests. External, customer-facing summary reports are produced by third party auditors can be made available upon request and under NDA. TT conducts monthly vulnerability scans of the infrastructure using automated tools. All identified vulnerabilities are tracked until mitigation with reports available for TT Operations management. Test results and other details are internal only.

Information Disposal

Data stored on media including hard drives and tapes are destroyed in a safe manner if they are defective. TT follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.

Appendix A: Ten Golden Rules for Information Security

1. Passwords are strictly personal.Your passwords are strictly personal and should be used exclusively by you in order to gain access to the systems concerned. Therefore, do not give your passwords to third parties or to a colleague and store them in a safe place, so not in your diary or on a yellow sticky note!

2. Reporting security incidents. It is important to report all security incidents to Compliance Manager as soon as possible.

Examples of incidents are a virus alert, a break-in or attempted break-in, or a door that should have been locked.

3. Duty of confidentiality.Within TT Customers' information is frequently used. Keep to the published guidelines as to how to deal with this.

4. Code of conduct,Internet and email use. Take care when using internet and email, avoid unsafe sites and do not open emails from unknown people.

5. Familiarizing yourself with the Information Security Policy. Within outsourcing, the Information Security Policy and accompanying guidelines are applicable. Familiarize yourself with these via your manager.

6. Providing information to third parties via the telephone.The key point is that requests for information by telephone about our customers will never be granted. That also means that no information about customers will be provided by telephone to people or organizations who claim to phone on behalf of those involved.

7. Clean desk / clear screen policy. Confidential treatment of customers' information includes, among other things, that each workplace is arranged in such a way that unauthorized people cannot access this information in your absence. That means that you should consciously lock your work station using the screen lock function whenever you leave your workplace. Neither is confidential information, such as files or reports, allowed to remain on your desk unattended or in a non-lockable cupboard. The printer is also a workplace; therefore, remove

customers’ information from the printer immediately following printing.

8. No confidential information in the waste bin.The correct treatment of confidential information –including customers' information –is very important within TT. Destroying this information should also take place in a safe way. Therefore, paper shredders or paper containers are available. Use these, and never put confidential information in the waste bin or in a container in your room destined for waste paper.

9. Approaching unknown people.Have you already been in the situation, that you encountered an unknown person in the room secured with security pass cards? Approach this person, introduce yourself and ask their reason for being in here. New colleagues, temporary employees or other hired staff appreciate being approached and in this way be able to make new contacts. However, people unauthorized to be in this space will be alerted to their infringement. Accompany these people to the person they wish to visit, or accompany them to the public part of the building.

10. Haste, stress, work pressure vs. information security. Information security does not come free –it costs energy and often works against you whenever you are in a hurry and when the work pressure is high. However, information security is extremely important for your work and is part of the professional and competent completion of the work. Therefore, take it very seriously –Customers of TT rely on this.