TUNGSTEN NETWORK LIMITED

GOVERNANCE & COMPLIANCE FRAMEWORK

Version 1.0

Document History			
Version	**Change Date**	**Author**	**Change Summary**
Draft	02-Sept-2015	C.Y. Hooi	Initial Design
1.0	01-Feb-2016	C.Y.Hooi	Final version

Definitions

Abbreviation	
ISMS	Information Security Management System
LRQA	Lloyd's Register Quality Assurance
SaaS	Software as a Service
GCD	Governance & Compliance department
Tungsten Network System	Tungsten Network's networks, websites, portals and extranets.
Information Assets	Information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), portal, extranet, intranet, PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

LAN	Local Area Network
SSL	Secure Socket Layer
AS2	Applicability Statement 2
VPN	Virtual Private Network
MAC	Media access control
HITECH	Health Information Technology for Economic and Clinical Health
Customers	Tungsten Network categories Customers as Buyers and Suppliers: Buyers mean customers who are connected to Tungsten Network and receive suppliers' invoices through Tungsten Network. Suppliers mean customers who send invoices through Tungsten Network to their respective buyers.
RTT	Ready to Transact
UAT	User Acceptance Testing
UCC	Unified Change Control form
VDI	Virtual Desktop Infrastructure
Security Sensitive Leaver	An employee who has access to sensitive systems, data or accounts or those leaving through disciplinary proceedings etc
Technical Operations team	Combination of Production Systems team and Internal Systems team

Table of Contents

1. Introduction

Tungsten Network ("the Company") understands that its reputation for maintaining confidentiality, integrity and availability is a valuable asset and is directly related to the compliance and conformance with International Standards, the Company policies and processes, countries legal and regulatory requirements in which the Company operates and clients contractual requirements.

Tungsten Network is committed to provide a consistent and reliable service by conforming to the International Standard on Assurance Engagements (ISAE) No. 3402. ISAE 3402 was developed to provide an international assurance standard for allowing professional accounting firms to issue a report for use by user organisations and their auditors on the controls at a service organisation that are likely to impact or be a part of the user organisation's system of internal control over financial reporting.

Tungsten Network is also committed to provide a secure service in a secure environment through complying and maintaining the ISO/IEC 27001 Standard Certificate. ISO/IEC 27001 is a specification for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. Organisations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.

It is Tungsten Network policy to conduct quarterly internal audits and reviews by the GCD on aspects of the physical, logical and process controls established as part of the ISAE 3402, ISO 27001 and HIPAA implementations across the business.

The purpose of this document is to provide a description to its audience on the compliance framework practiced by Tungsten Network to ensure that the Company maintains the ISAE3402 Type 2 Audit Report and ISO27001 Certificate. Each of these standards requires Tungsten Network to demonstrate compliance and conformance towards different sets of controls.

2. Governance & Compliance Structure

Tungsten Network's GCD is part of the Tungsten Corporation Legal department, reports to the General Counsel and is therefore fully independent to the business. The GCD is also part of the Tungsten Network Data Security Committee and is required to assist with steering, maintaining and improving the Tungsten Network ISMS.

3. Measurement & Improvement

Tungsten Network Management understands the importance of reviewing the way it performs its process and security audits to ensure they remain effective and that lessons learned from previous audits are included in policy and process revisions.

Tungsten Network Management appreciates the value of receiving an independent and non-bias review on the Company's governance posture from a third party audit. All elements within the ISAE 3402, ISO 27001 and HIPAA implementations will be audited by a third party at least once a year as required by the standards and the GCD is responsible to facilitate these audits to ensure that the third party auditor receives all the necessary resource and material.

The general effectiveness of the controls is measured through the internal and external audit programs by having 0 major non-conformances and less than 15% minor non-conformance findings in the overall controls being audited. Nonconformance is justified as a non-fulfilment of a requirement required by the controls in this document confirmed through interviews, observations and sampling. Any exceptions discovered during an audit will be registered in the nonconformance tracker. The purpose of the nonconformance tracker is to enable GCD to centrally store and track nonconformities, agreed mitigation, timeline and mitigation progress. The nonconformance tracker is an internal document maintained by the GCD only. No exception can be left untreated unless it is accepted as part of the risk assessment signed off by the Chief Operating Officer.

4. Training and Awareness

Tungsten Network provides training and awareness to ensure that all employees are aware of and implement policies and processes which are related to their roles.

Tungsten Network line managers must ensure all members of their department are aware of policies and processes required to do their role.

The GCD is responsible for identifying suitable information security training materials to enhance employees' knowledge on cyber-attack methods. The training is also to enable employees to identify and to avoid common threats like phishing and social engineering.

The GCD also initiates periodic assessments to ensure that the Company policies and processes and relevant updates are communicated to all staff.

5. Risk Management

Tungsten Network approach to risk is described in the risk management framework which applies to the overall strategic planning process of the business. The risk management framework is designed to identify and assess risks (including information security risk) in the business plan on an annual basis. The purpose of the risk management framework is also to identify and evaluate options for the treatment of those risks, and to select control objectives and controls that will reduce those risks to acceptable levels within the context of the business plan, operational requirements, constraints and objectives and international legislation and regulation.

A risk registry is maintained and reviewed on an annual basis by the Data Security Committee. The risk registry is kept up to date with emerging risks being added as required and mitigating actions and controls being updated as necessary.

Risks are determined by the likelihood and impact of threats and vulnerabilities of assets. Controls are selected and approved by the Data Security Committee to mitigate risks.

The table below includes timescales for guidance only, actual timescales and actions to be taken will be decided and prioritized by the Data Security Committee.

Risk Level	Action	Review (until mitigated)
Low	• No action required	N/A
Medium	• Need to be treated by remediation or transfer • Can be accepted by Risk Owner	Half Yearly
High	• Need to be treated by remediation or transfer • Can be accepted by Risk Owner • Risk acceptance must be approved by Data Security Committee	Quarterly
Critical	• Need to be treated by remediation or transfer • Can be accepted by Data Security Committee	Monthly

The Risk Calculation Table below is practiced by Tungsten and uses a four point (Critical, High, Medium and Low) scale for labelling the likely-hood and impact of threats and vulnerabilities. Each asset owner judges the risk based on five severity scales for likelihood and impact.

Risk Calculation:

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Risk Level:

Low	Level 1	Medium	Level 2	High	Level 3	Critical	Level 4

All risks that are at or below Medium risk level can be accepted by the risk owner. Risks that are at a level higher may be transferred to a third party such that the residual risk is at or below the accepted level, or must be reduced by implementation of appropriate controls to a level consistent with the risk acceptance criteria. Where necessary, additional controls will be selected and implemented in order to reduce the residual risk level below the acceptable level. Wherever residual risk remains for any reason above the acceptable risk threshold, senior management approval must be provided for that level of exposure.

More details are available in the Risk Management Policy.

6. Change Management

Tungsten Network change management applies to all changes on the Production systems performed by Tungsten Network employees and third parties acting on behalf of Tungsten Network. All changes need to be assessed for risk, registered and implemented in a manner which provides a stable operational environment to minimize the potential impact. Tungsten Network change management has classified 4 different risk levels based on the estimated change impact on the production environment. Each risk level will require different supporting document or information and level of approval.

Prior to submitting a change request for approval, the change requestor is required to plan, build and test the change. Once these are done, the change requestor is required to complete the UCC and prepare all necessary supporting documents. Supporting documents also involve a rollback plan for quick recovery in case of fail change.

The completed UCC is submitted to Ops Coordination for approval process. The approval process involves reviewing the UCC and its supporting documents for completeness, ensuring risks are correctly assessed and engaging relevant asset owners to review and approve the change request. A change request cannot be approved by the change requestor and must be approved by the owner of the asset where the change will be applied onto. Applying a change to the production environment can only be performed by the Production team and deployed at a time that will cause the least inconvenience to users, preferably out of hours or during non-core hours or agreed maintenance windows whenever possible.

More details are available in the Change Risk Assessment and Application Policy

7. Incident Management

Tungsten Network recognizes that it is possible to experience an incident during the normal course of business that either impacts, or threatens to impact, the normal running of the business. Tungsten Network will investigate on all reported incidents whether it is an actual or suspected incident and react quickly and effectively towards an actual incident in order to ensure that the impact to the business is as minimal as possible.

All confirmed incidents will be managed in accordance with the Tungsten Network incident management process whereby an incident manager will be appointed and relevant department members will be nominated to form the incident management team. The incident management team is responsible for ensuring the recovery of an incident, the continuation of the service, and for all communication to the Company and Customers.

A detailed incident report will be produced for all actual major incidents and stored for a minimum of two years. Tungsten Network's incident reporting policy is also compliant with HITECH breach notification regulations.

More detail is available in the Incident Management Policy and the related process documentation.

8. Customer Integration

The purpose of the Customer integration process is to ensure procedures are adhered to before Customers can be integrated into the Tungsten Network system and that Customers are satisfied with the Tungsten Network service. The process ensures that:

- Service contracts are signed between Customers and a Tungsten Network authorized signatory.
- An e-service contract can also be signed via the Portal for certain Customers.
- The Integration process only begins after a service contract is signed.
- Customers' requirements for integration are fully captured and implemented onto Tungsten Network services.
- Customers' complaints and discrepancies are resolved accordingly.
- Customers are only categorized to RTT after they have approved the UAT.

Adherence to the above process is mandatory to ensure the successful technical integration of each Customer to Tungsten Network and thereby enables the Buyer to electronically receive invoices into their accounts payable system. The process involves 'mapping' Buyer requirements into the Tungsten Network System that enables creation of data and invoice image files when a Supplier submits an invoice through Tungsten Network..

The integration process is controlled and completed in-house at Tungsten Network's offices using internal workflow applications. The mapping process is controlled by Tungsten Network's staff using internal tools for developing the Customer mapping requirements.

More detail on Customer Integration is available in the ISAE 3402 Report.

9. Technical Operations

Tungsten Network's e-invoicing services are required to be operational and conforming to the clients' requirements. The Technical Operation's team manages the Company technology operations to meet the requirements of the clients, including the use of third parties in completing

these activities. The team is segregated into two sub-teams with separate roles and responsibilities. More details on Technical Operations is available in the ISAE 3402 Report.

9.1. Production Systems Team

The Production team is responsible for the monitoring, maintaining and troubleshooting of applications that are hosted in the datacentre. These applications are Tungsten Network's business critical applications such as the Tungsten Network services connectivity, core applications and database.

The daily operations of the team involves troubleshooting escalated tickets related to Production Systems services such as invoice processing to ensure Customers are able to send and receive invoices without undue delay (Section 9.3: Invoice Processing). The Production Systems team is also responsible for managing the Tungsten Network datacentre service providers (Section 10.1: **Error! Reference source not found.**).

Security in the Production System is also a critical aspect of Tungsten Network and therefore security controls related to the Production Systems are strictly governed by the GCD. The following are some of the security controls governed in the Production systems:

- Access Control
- Cryptography Control
- Physical and Environmental Control
- Backup Control
- Technical Vulnerabilities Control
- Network Security Management
- Suppliers Relationships Control

The controls above are further explained in Tungsten Network Information Security Governance of this document.

9.2. Internal Systems Team

The Internal Systems team of Technical Operations is responsible for managing user access, server room and IT assets and infrastructures for Tungsten Network's corporate offices. The Internal Systems team is also responsible for managing the environments which host all business critical internal tools. There are tools which other functions within Tungsten Network relies on to deliver their day to day operations. Customers' sensitive information are not stored in these environments or tools.

The Internal Systems is also obligated to adhere to security controls set forth by the Company and governed by GCD. The following are some of the security controls governed in the internal systems:

- Access Control
- Asset Management
- Mobile Devices and Teleworking Control

- Protection from Malware
- Backup
- Network Security Management

The controls above are further explained in Section 11 of this document.

9.3. Invoice Processing

Once Customers have been successfully integrated into the Tungsten Network, the on-going processing of invoices is an automated activity with monitoring and support services provided by Tungsten Network. There are 3 key invoice processing stages that need to be operating as intended to ensure successful completion of the transaction by Customers:

› Key Stage 1: Invoice receipt and Validation

At this stage, Tungsten Network systems will validate invoice data submitted by Customers to confirm if it satisfies the necessary invoice requirements. The system will reject the invoice and send an automated email to Customers if the invoice fails to pass this stage.

› Key Stage 2: Invoice Processing

At this stage, the system validates that invoices submitted by Customers are processed in accordance with the agreed file format and timelines. Invoices that fail any validation will be rejected by the system and an email will be automatically sent to the Customer with a reason code. Customers may contact Tungsten Network Support through the ticketing system if they need assistance with a rejected invoice.

On a daily basis, the support team will also check for invoices that have passed the validation process but still have not been delivered. This scenario is usually caused by various reasons that requires the support team to investigate and identify the reason. Once the root cause has been identified, the support team will proceed to remediate the problem or escalate it to another relevant team if needed for remediation.

› Key Stage 3: Invoice Delivery

After an invoice has successfully passed the Stage 1 and 2 process, the system delivers the invoice data and image files processed to the intended Customers.

More details on Invoice Processing are available in the ISAE 3402 Report.

10. Managed Services: Outsourced IT Operations

Tungsten Network outsources its datacentre services which host its entire Production systems and database in the United Kingdom. The Company also uses Amazon Web Services (AWS) in the United States to host its database for US Customers that requires strict compliance with HIPAA or related legislations. The management of AWS is also outsourced to an US based datacentre service provider. The company's development team engages a third party software development company (Luxoft) to assist them in developing, enhancing and maintaining the Company Core

Systems. These service providers are required to acknowledge and adhere to security controls defined by Tungsten Network for all its suppliers (Supplier Relationships).

More details on Managed Services: Outsourced IT Operations is available in the ISAE 3402 Report.

10.1. Datacentre

Tungsten Network engages two Technology Service Providers to manage its US and EU platforms respectively. US Technology Service Provider provides a managed service on Tungsten Network AWS production environment. The EU Technology Service Provider provides physical datacentre hosting and a managed service that covers:

- Provision of datacentre facilities
- Virtual Private Network configuration on managed devices located within the hosted infrastructure
- Application management
- Incident problem and change management
- Hardware and software patch management
- Test and release management
- Back-up and storage
- Secondary disaster recovery site

As Tungsten Network Core system and database are hosted in United Kingdom, the GCD performs a physical audit on the datacentres on a yearly basis. Customers can request for Tungsten Network and its datacentres ISO27001:2013 Certificate.

10.2. Software Development

Tungsten Network engages an off-shore software development contractor that provides Tungsten Network with software development and support services involving Tungsten Network core systems. The development contractor is contractually bound to comply with strict software development security controls set forth by Tungsten Network and audited by GCD. All builds developed by the development contractor are required to perform code reviewed and tested by Tungsten Network development team. These security controls are further explained in Section 11.10 of this document.

11. Tungsten Network Information Security Governance

Tungsten Network Management has chosen ISO27001 standard for Information Security Management System (ISMS) as the most appropriate way of formalizing the Company's approach to data security and as a key mechanism for flowing down the responsibilities that all employees have in ensuring that Customers trust is well placed. Tungsten Network employees' commitment to this is crucial, and is one way in which the employees can help the Company to achieve its vision of becoming the most trusted global trading network.

Tungsten Network Management has established the Data Security Committee ("The Committee") and defined its responsibility in maintaining the ISMS providing guidance on its implementation, and ensuring compliance at all times.

11.1. Information Security Policy

It is the policy of Tungsten Network to preserve the availability, confidentiality and integrity of its information assets which also applies to partners that are part of the integrated network and have accepted Tungsten Network's security undertakings. Tungsten Network Management has established the following as its security policy:

- Information will be protected in line with all relevant Tungsten Network policies and legislation, notably those relating to data protection and human rights.
- Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate use of the asset and ensuring that appropriate security measures are in place to protect the asset. Asset users are also bound by Tungsten Network asset management & classification policy.
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The availability, confidentiality and integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification and according to the training they have received.
- Tungsten Network will use appropriate measures in order to protect information assets to ensure they are protected against unauthorised access. This will include physical, technical and contractual measures as deemed appropriate for the asset.
- Compliance with the information security policy will be enforced by Tungsten Network Management

More details are available in the Tungsten Corporation Security Policy.

11.2. Organization of Information Security

11.2.1. Internal organization

The Committee is responsible for defining Tungsten Network's information security policy and for ensuring it is discharged by all departments through Heads of Departments. The Committee carry out the duties below for the Company, its major subsidiary undertakings and the group as a whole, as appropriate:

- Members of the Committee will provide advice in matters related to their areas of expertise.
- Coordinating and directing Tungsten Network security framework.

- Commissioning or preparing information security policy statements, ensuring their compliance with the principles and axioms approved by the Tungsten Network Management and formally approving them for use throughout.
- Periodically reviewing the security policy statements to ensure the efficiency and effectiveness of the information security controls infrastructure as a whole, recommending improvements wherever necessary.
- Keep under review the adequacy and effectiveness of the Company's risk management system in relation to the Security of Information for Tungsten Network.
- Identifies significant trends and changes to Tungsten Network information security risks and, where appropriate, proposing changes to the controls framework and/or policies for example by sponsoring major strategic initiatives to enhance information security.
- Reviewing major security incidents and, where appropriate, impose strategic improvements to address any underlying root causes.
- Reviewing major non-conformance finding on internal and external audits and, where appropriate impose strategic improvements to address any underlying root causes.
- Reviewing medium to high risk finding on internal and external risk assessment and, where appropriate impose strategic improvements to mitigate risk occurrence

More details are available in the Data Security Committee Terms of Reference.

11.2.2. Mobile devices and teleworking

Tungsten Network provides telephone and mobile devices to employees to allow them to perform their role in the business. The Company telephone and portable device usage policies mandate all employees to be responsible for their own usage of these devices and the activities they conduct with them. Employees are required to ensure any transfer or disposal of these devices follow the proper process. Misuse of devices such as the following have serious consequences and may lead to disciplinary measures being taken:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene or pornographic;
- Defamatory or threatening;
- In contravention of copyright laws;
- In contravention of civil or criminal law; and
- In contravention of any Tungsten policies.

Tungsten Network also provides remote access connectivity flexibility to employees with business needs. Employees are able to access their emails and internal tools and documents whenever and wherever for business purposes. The remote access connections to Tungsten corporate network are secured through a VPN tunnel. Only equipment provided by the Internal Systems team or individual equipment approved by the Internal Systems team leads are allowed to have VPN access.

More details are available in the Telephone Network Computing Equipment Usage Policy and Remote Working and Portable Device Usage Policy.

11.3. Human Resource Security

The Tungsten Network Human Resource (HR) department is overall responsible for human resources process and security. HR is responsible for ensuring that recruitment activities are appropriately logged and tracked. They will place vacancies with agencies or advertising them directly. Managers wishing to place vacancies themselves are required to consult with the Human Resource first.

Candidates are selected by respective line managers and jointly interviewed together with a human resource personal. Prior to new employees, agents and temporary employees begin working in Tungsten Network premises, line managers are required to submit a starter form if they need access to Tungsten Network Information Assets. Their level of access and the resources provided is based on the role they are performing as approved by the line manager.

In order to comply with legislative and company insurance requirements, a valid signed contract covering the period of employment needs to be in place prior to the person begin working in Tungsten Network premises.

Changes to an employee's role necessitating a change in access rights must be made according to the standard groups created. If access to resources outside this job function is required then approval from the line manager and the Information Asset owner is required.

Upon the termination of employment, the employee's line manager or a member of the HR team must notify the Internal Systems team via a leaver notification form. If the employee is classed as a security sensitive leaver, they must return all Tungsten Network property immediately upon request otherwise it must be returned by the end of the business day on their agreed leaving date. All items must be returned to Internal Systems, even if the employee is keeping elements of the equipment for verification and data removal.

More details are available in User Setup and Removal Policy, Code of Conduct and Recruitment Policy.

11.4. Asset Management

11.4.1. Responsibility for assets

All Tungsten Network assets received by the company are tagged with a unique identifier whenever possible. The asset registry will be updated with the unique identifier and the initial location/allocation of the asset. Assets which are transferred to a different geographic office location will be reassigned to the appropriate asset register. When an employee with individually assigned assets leaves the company the assets status are reflected on the asset register. The Company strictly manages all of the physical assets used within the business which could contain valuable data to ensure that:

- All physical assets are identifiable and traceable
- Users of Tungsten Network Information Assets are required to sign and adhere to the System Rules of Behaviour.
- End-of-life planning is taken into account during budgetary processes to ensure an effective replacement process
- Assets containing or potentially containing Information Assets are securely cleansed of data prior to disposal at end-of-life or as a result of premature removal from Tungsten Network control

More information is available in Asset Management & Classification Policy.

11.4.2. Information classification

Tungsten Network enforced an information asset classification process that systematically grades information against a set of criteria to determine the levels of accessibility, security and redundancy. All Tungsten Network employees and agents are responsible for exercising due care in their use of, and protection of information. Unauthorized disclosure howsoever caused may be dealt with under the company's disciplinary procedures. Employees and agents are also responsible for ensuring all information distributed via electronic or printed means are covered by appropriate disclosure agreements and/or contain approved confidentiality notice. Information are categorised as:

- Class 1: Standard
- Class 2: Medium
- Class 3: High
- Class 4: Secret

As a general rule of Tungsten Network information security requirement, all clients' data that are not publically available are categorised as Class 2 information.

More information is available in Asset Management & Classification Policy.

11.4.3. Media handling

Tungsten Network enforces strict controls on usage of storage media and clients information. Employees are prohibited to copy any Company digital information assets to any non-Tungsten Network external storage media.

The Company also mandates all employees to store clients' information on Tungsten Network Corporate environment. The Corporate environment is restricted to with access control and remote access via VPN.

All critical documents are only allowed to be stored in the Corporate or Production servers where it is protected through certified logical and physical security controls.

Backup media stored on-site are kept in a secure area away from the back-up device. Access to the area is restricted to approved personnel only. Backup media stored off-site is provided by a third

party service provider. The service provider site includes fire suppression systems, checking in/out process and secure storage. Backup media are encrypted or password protected when encryption is not possible before it leaves Tungsten Network office.

Damaged, retired, or obsolete media are disposed of in a secure and approved manor. This is completed via either an approved service provider or the media being manually destroyed through dismantling.

More information is available at Remote Working and Portable Device Usage Policy

11.5. Access Control

Tungsten Network provide all employees and other qualified users with the access to information they need to carry out their responsibilities through request, review and approval control. Line managers must complete and submit the starter form to request for access for their new employee. The form will be reviewed by Human Resource and Ops Coordination before Technical Operations team creates the account. Password is forced to change upon first login through Tungsten Network active directory policies.

Privilege access level are only given to Technical Operations team, any other department that requires a privilege access for its member will have to make a formal request to Ops Coordination teams for approval before the access level is granted by Technical Operations team. The privilege access level or the account depending on the situation will be removed immediately once it has accomplished its intended purpose.

Internal Systems team is responsible in managing all user access request related to Tungsten Network corporate environment while the Production Systems team is responsible in managing all user access request related to Tungsten Network production environment.

More information is available at Network Access Policy and User Setup and Removal Policy.

11.6. Cryptography

11.6.1. Cryptographic controls

Tungsten Network provides some of the best practices for encryptions for protection of confidentiality, integrity, authentication of information. Tungsten Network also ensures that the use of encryption technologies conforms to relevant applicable requirements. The following are the types of cryptography control used to protect clients' data when transferring data through Tungsten Network:

- SFTP
- FTPS
- AS2 (via HTTPS)
- HTTPS
- FTP/HTTP utilizing file level encryption (PGP)
- VPN tunnel

In each of the above scenarios, private keys will be managed by the Technical Operations team. Public keys will be made available for client facing implementation and support teams to relay to clients when configuring the encryption as needed.

Any website containing confidential information is accessible via a TLS encrypted channel only and verified by a certificate issued by a credible third party certificate authority.

Digital certificates are only accessible by the Technical Operations or Web Services management team. Access to digital certificates are secured on the corporate network and access restricted only to users requiring access to them to deploy to web servers.

Data at rest on servers are encrypted when possible and data backed up to removable media such as tapes should be encrypted.

More information is available at Cryptography policy.

11.7. Physical and Environmental Security

11.7.1. Secure areas

All Tungsten Network office environment uses some form of physical token to grant access and these are controlled to ensure traceability. Where practical, CCTVs are installed to act as a further deterrent and also to provide an investigative means.

Each office has at least one nominated access controller responsible for controlling access to the building through a controlled issuance of access tokens. Access controllers are responsible for maintaining a record of the access tokens issued/returned/lost/stolen and the available stock.

Important equipment are carefully placed and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Employees are responsible for their visitors and must ensure they are accompanied at all times within the office environment. Visitors are not permitted into restricted areas unless approved by Tungsten Network management.

Access into and out of the office server room is managed by the Internal Systems manager or respective team leads. The primary mechanism for controlling access to the office server rooms is via token access restricted to Internal Systems team personal and employees approved by Tungsten Network senior management only.

Business critical equipment are situated in the production environment hosted in a tier 3 datacentre located in Europe and the datacentre service is provided by a service provider. The datacentre physical security is controlled, managed and maintained by the service and Tungsten Network will audit its effectiveness annually.

More information is available at Building Access Policy.

11.7.2. Equipment

Tungsten Network Internal Systems team performs daily checks on major corporate equipment to ensure availability of processing facilities service. Employees are responsible to contact the respective Internal Systems team on any issues related to their IT equipment.

Corporate server room equipment are protected from power failures and other disruptions caused by supporting utilities failure such as UPS, manual power disconnect, fire protection system and air conditioning. Corporate office power and telecommunications cables are protected from unauthorised use or damage.

Equipment located in the datacentre is maintained and secured by the datacentre service provider and Tungsten Network assesses their service level through monthly service report and annual audits.

11.8. Operations Security

11.8.1. Operational procedures and responsibilities

Tungsten Network policies are fully documented and accessible to all employees. Tungsten Network management also mandates process owners to formally document and maintain their department operational procedures with the assistance of GCD. Creation, change, removal and approval of policies and process documents are controlled through Tungsten Document Control policy. The availability and accessibility of these documents are enhanced through Tungsten Network online document library. A separate editable copy of these documents are kept in the Company file server GCD folder accessible only by GCD members.

More information is available in Documents Standard Policy.

11.8.2. Protection from malware

All Tungsten Network processing facilities and their underlying infrastructure are protected from threats posed by malicious codes, viruses and Trojans through the use of antivirus software on IT devices and the controlled usage of equipment and facilities by employees. All corporate environment servers accessible by users and public facing servers are installed with an approved antivirus software. Virus patterns/detections are updated automatically by the antivirus central management server whenever a Company device connects onto the Company network. Full scans on processing facilities are performed at least once a week outside of normal working hours.

More information is available at Anti Virus Policy.

11.8.3. Backup

Information Assets are predominantly stored on Tungsten Network production environment and the corporate environment infrastructure. Backups are performed every day and where it is likely that significant amount of data have changed. Full backup are performed for each server when possible. When a full backup is not possible, an incremental will be used to provide the best possible protection. Corporate environment backup data are transferred offsite on a weekly basis

while the production environment backup data are real-time mirrored to the secondary disaster recovery datacentre.

GDC initiate the backup recovery testing with Production Systems team on a monthly basis and the Production Systems team is required to provide GDC with the necessary evidence of completion.

More information is available at Data Backup Policy.

11.8.4. Logging and monitoring

Tungsten Network protect its information assets hosted in the production environment against the consequences of breach in confidentiality, failures of integrity or disruption to the availability of information through loggings and monitoring of user and system events. Tungsten Network has implemented monitoring tools to provide real-time alerts and weekly reports on various labelled activities on the production environment. Tungsten Network GCD, Production Systems team and datacentre service provider utilizes individual monitoring tools on the production environment. Events flagged as potentials by the tools will be actioned upon as a preventive measure .Audit logs are kept for at least 90 days.

More information is available at Information Security Monitoring Policy.

11.8.5. Control of operational software

Tungsten Network limit its IT assets to allow operational software that are required for business needs only. This restriction is enforced through user access management where all employees are given normal user access level only which limits installation of software and usage of administrative tools on work devices. Employees requiring to install additional software need to make a request to Internal Systems. Once Internal Systems reviewed and accepts the software, Internal Systems personal will manually installed it onto the requestor workstation.

11.8.6. Technical vulnerability management

Tungsten Network performs vulnerability scanning on all internet facing services and network devices to ensure vulnerabilities are identified and managed in a timely manner. All detected vulnerabilities will be mitigated by Technical Operations or Web Development respectively facilitated by GCD to ensure completion. The following are the types of vulnerability scans that Tungsten Network performs on its systems:

No.	Scan Type	Scan Period
1	External Penetration Test	Half-Yearly
2	Internal Devices Vulnerability Scan	Weekly
3	Internal Services Vulnerability Scan	Weekly

4	Source Code Review (Static and Dynamic)	Quarterly & Every Deployment

GCD is responsible to report and track the above results in accordance to the scan period with Technical Operations and Web Development Team respectively. GCD will categorise the findings into 4 categories:

No.	Categories	Mitigate Period	Acceptable Risk
1	Critical	1 Month	N
2	High	1 Month	N
3	Medium	3 Month	N
4	Low	6 Month	Y

Technical Operations and Web Development team are responsible to mitigate the reported vulnerabilities within the stipulated time above. Vulnerabilities detected on Tungsten Network web applications must be mitigated by Web Development Team. GCD team will escalate any vulnerability that fails to be mitigated within the stipulated time to Data Security Committee for further action.

More information is available at Information Security Monitoring Policy.

11.9. Communications Security

11.9.1. Network security management

Tungsten Network restricts access to its production and corporate network infrastructure and control devices permitted to access the network. Only devices conforming to the Company configurations standard may access the corporate network or the production network. The production network is restricted to only Productions team and personal approved by senior management and Director of Technical Operations and Systems. Inactive sessions on the production network and relevant applications will be shut down after a defined period of inactivity.

Firewall controls are in place between DMZ and internal networks to prevent access on non-required ports and protocols. This is to also to ensure that computer connections and information flows do not breach to Tungsten Network access control policy as applied to the business applications.

11.9.2. Information transfer

Tungsten Network mandates that any confidential information shared with employees, sub-contractors or third parties of any description be the subject of a confidentiality agreement. All Tungsten Network employees and contractors are required to acknowledge and sign the System

Rules of Behaviour form before they are given access to Company processing facilities and assets. The Company also mandates that all customer information must be treated as confidential information requiring protection under a non-disclosure agreement. Customer or supplier NDA to the Company must be reviewed by the Legal department and can only be signed by the authorized personal of Tungsten Network before it is considered effective.

Tungsten Network protect its network transportation through various security mechanisms such as TLS, AS2, VPN and such. Tungsten Network employs a certified PCI Level 1 Service Provider to process all its credit card transactions.

11.10. System acquisition, development and maintenance

11.10.1. Security requirements of information systems

Tungsten Network categorises any implementation whether it is a new service or serve as an upgrade to the existing services as a change to the systems that needs to be regulated by the Company Change Management mentioned in Change Management of this document. The Company governs strictly all changes to its infrastructure through the change management control. All changes will have to be assessed for risk, registered and implemented in a manner which provides a stable operational environment in accordance to the change management to minimize the potential impact.

11.10.2. Security in development and support processes

Tungsten Network applies Agile Scrum methodology on its development as opposed to the traditional System Development Life Cycle ("SDLC") based Waterfall model. The Agile Scrum methodology practiced by the Company Development team is broken down into 5 phases:

- Phase 1: Requirements gathering
- Phase 2: Planning
- Phase 3: Analysis, design, development and testing
- Phase 4: Review, release and maintenance
- Phase 5: Release process

Addressing security elements associated with the coding of any Tungsten Network related web applications begin in the early stage of the SDLC at Phase 2: Planning. The Company Development team, Testing team and any other employee that is involved in coding development of any Tungsten related web applications are required to apply coding best practices to ensure that security is part of development projects. The secure coding practice that is recognized by the Company is the Open Web Application Security Project ("OWASP") Top 10. The OWASP Top 10 represents a broad consensus on the most critical web application security flaws. The errors on OWASP Top 10 list occur frequently in web applications, are often easy to find, and easy to exploit.

All development builds are required to be code reviewed with a third party scanning tool before being deployed on to the Production environment. Any medium and above findings detected during the scan will need to be addressed before a build can be accepted for deployment.

More information is available at SCRUM SDLC document.

11.10.3. Test data

Tungsten Network forbids the use of live data to be used on the testing environment. The Testing team develops its own testing script, test case and test data for testing purposes.

11.11. Supplier Relationships

11.11.1. Information security in supplier relationships

Tungsten Network requires its third party to demonstrate commitments before entering a contract with them and also during their tenure of service delivery. The Company categorises its third party in to three categories based on a vendor category calculation matrix:

- Critical vendor
- Standard vendor
- Casual vendor

Each category have a different set of requirements to fulfil and any non-compliance to these requirements will require remediation action from the vendor or Tungsten Network senior management to accept the risk. Failing in either one can lead to contract termination or third party being rejected during the selection process. Upon the termination of a contract or agreement with a vendor, or in the event of un-waived compliance issues, all vendor access will be removed along with all related user accounts. Reports and audit logs related to the vendor will be kept for a minimum of 12 months.

Approved vendor that requires connection to Tungsten Network Corporate or Production network will need to complete the following before they are allowed access:

- Vendor to complete Tungsten Network Third Party Access Request Form
- Vendor connecting to Tungsten Network's network with their own devices will need to have their devices verified by Internal Systems team prior to granting access
- Vendor connecting to Tungsten Network's network with Tungsten Network device will need to sign the System Rules of Behaviour form. Certain requirements in the form may be exempted by the Head of Network Compliance

Approved vendor that are allowed access to Tungsten Network corporate and production network can only connect through the following methods:

- Secure VPN with IPSEC via Cisco client for third party individual user access
- Secure access to a virtual desktop infrastructure (VDI) over HTTPS for third party individual user access
- Secure site-to-site VPN with IPSEC for entire third party site

Service provider that falls under the Critical Vendor category will have their service reviewed by GCD on an annual basis or whenever Tungsten Network chief operating officer deemed necessary to do so.

More information is available in Third Party Control policy and Third Party Access Control.

11.11.2. Supplier service delivery management

Tungsten Network executive manager(s) responsible for the area of contracting the vendor is overall responsible for ensuring the fulfilment of the control mentioned in 11.11.1 of this document and manage vendor service delivery competency. Vendors are required to submit their monthly service report to the Tungsten Network executive manager for service level agreement measurement. GCD will randomly select these reports for compliance assessment during the quarterly audits.

11.12. Compliance

11.12.1. Compliance with legal and contractual requirements

Tungsten Network is committed in complying with all required legislation as part of its on-going business activities. As the company utilizes and processes a wide variety of Information Assets from multiple countries as part of its business activities, many of which are governed by regulatory requirements. As such, Tungsten Network Legal department is consistently maintaining awareness of regulatory changes effecting Information Assets and implementing appropriate solutions in order to remain compliant.

More information is available in Regulation Compliance Policy.

11.12.2. Information security reviews

Tungsten Network is committed in maintaining and where possible improving its information security management systems to safeguard its Information Assets. GCD initiates quarterly internal audit programs to ensure that all documented policies, and work instructions are carried out as mandated by the Company management.

GCD is also tasked to ensure the Company information processing facilities are technically compliant with international security standards through facilitating all penetration scans and vulnerabilities mitigation works.

More information is available at Effectiveness Measurement and Audit Policy.