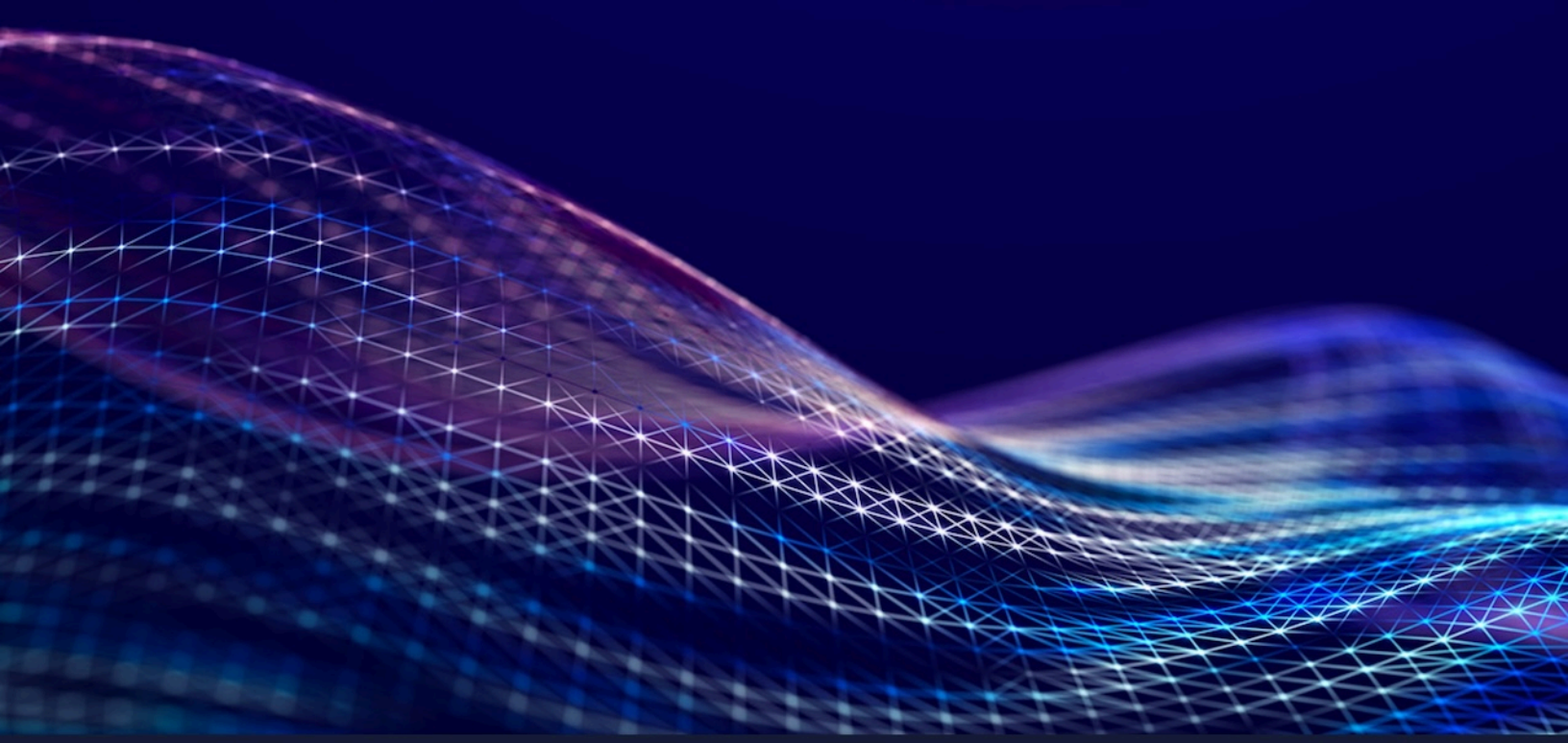


Tungsten Automation

Security and Compliance Guide

2025.3

TUNGSTEN AUTOMATION

Contents

Preface

This guide describes how Tungsten Automation addresses security and compliance by securing personal and confidential information. This document also contains essential information about requirements related to the Payment Card Industry Data Security Standard (PCI DSS), the Protected Health Information (PHI) regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the General Data Protection Regulation (GDPR) implemented by the European Union (EU), and the California Consumer Privacy Act (CCPA) legislation enacted by the State of California.

Note: Information in this document is based on current Tungsten Automation Products. Please consult your Tungsten Automation professional for additional features and functionality.

Terms and Definitions

Active Directory (AD): Technology created by Microsoft to provide a centralized and standardized system that automates network management of user data, security and distributed resources, and enables interoperation with other directories.

Advanced Encryption Standard (AES): National Institute of Standards and Technology specification for electronic data encryption based on the substitution-permutation network principle.

California Consumer Privacy Act (CCPA): Privacy law enacted in 2020 by the State of California. The law includes regulations granting California consumers data privacy rights and control over personal information, including the right to know, the right to delete, and the right to opt-out of the sale of personal information collected by businesses. The law also includes protections for minors.

Encrypting File System (EFS): File system-level encryption used to encrypt data from attackers with physical access to the computer.

Federal Information Processing Standards (FIPS): Provides increasing qualitative levels of security covering a wide range of potential applications and environments where cryptographic models can be applied.

General Data Protection Regulation (GDPR): Data protection law implemented by the European Union (EU). The law imposes strict rules for institutions and entities who process and host personal data worldwide. Institutions, businesses, and individuals outside of the EU must also abide by the regulations when they collect or process data for any EU citizen.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): An act created by the U.S. Congress that ensures individual health care data is accessible, portable, and updatable. This act sets standards for medical data sharing across the U.S. health system to prevent fraud.

Hypertext Transfer Protocol Secure (HTTPS): The use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sub layer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests and the pages that are returned by the Web server.

IPsec: Internet Protocol Security authenticates and encrypts each Internet protocol packet of a communication session and is used to protect data that flows between a pair of hosts or networks.

MD5 hash (message-digest algorithm): Data verification method that uses a cryptographic hash function to produce a 16-byte hash value. Used in a wide variety of cryptographic applications.

Payment Card Industry Data Security Standard (PCI DSS): Standard that governs security requirements for processing payment card data. Its use is mandated by all the major payment card companies.

Protected Health Information (PHI): Also referred to as Personal Health Information; includes patient medical records, health care payment details, health care information, and individual health status.

RSA: Uses public and private key encryption where the encryption key is public and differs from the decryption key.

Server Message Block (SMB) Protocol: Provides a method for client applications on a computer to read and write to files on and to request services from server programs in a computer network. This protocol can be used over the Internet on top of its TCP/IP protocol or on top of other network protocols such as Internetwork Packet Exchange and NetBEUI.

Security Identifier Definition (SID): A unique numeric identifier to identify a security principal or group in Windows operating systems.

SQL Encryption: Hierarchical layered data encryption that can include symmetric and asymmetric keys and certificates to encrypt data in the database.

SSL: Secure Sockets Layer is a certificate-based cryptographic protocol that provides encrypted communication and authentication between two entities over the network during transit**.**

SSO: Secure Single Sign-On.

Syskey: Utility used to encrypt hashed passwords using a 128-bit RC4 encryption key.

Transport Data Encryption (TDE): Technology employed by both Microsoft and Oracle to encrypt database files. TDE offers encryption at the file level. TDE solves the problem of protecting data at rest, encrypting databases both on the hard drive and consequently on back-up media.

Transparent Layer Security (TLS): Transport Layer Security is a certificate-based cryptographic protocol that provides encrypted communication and authentication between two entities over the network during transit.

Overview

Tungsten Automation customers provide products and services for industries in the healthcare, financial services, government, and other sectors of the global economy. As such, they are subject to regulations that directly impact the security requirements for Tungsten Automation Products. The most common regulations affecting customers are summarized in the following table.

Regulation	Industry	Description
HIPAA	Healthcare	The U.S. Health Insurance Portability and Accountability Act of 1996. Corporations have to identify PHI at risk for unauthorized disclosure, and implement encryption as a security control to avoid breach of disclosure requirements.
Data Breach	Financial Services	A data breach is a breach of security leading to the unauthorized disclosure or alteration of personal data stored or transmitted by providers of electronic communication services. In the case of a breach, the provider must notify the competent national authority of its occurrence "without undue delay."
PCI-DSS	Financial Services	The Payment Card Industry (PCI) Data Security Standards. Specifies the security controls that companies accepting, transmitting, or processing credit or debit card payments must have in place if they are involved in accepting or processing online credit card payments.
ISO/IEC 27001	General	Formally specifies a management system that is intended to bring information security under explicit management control.
FIPS-140	Government, Financial Services	Specifies specific encryption algorithms and implementations that have been certified by NIST.
GDPR	General	Data protection laws for EU Member states and provides strict rules for institutions and entities who process and host personal data worldwide.
CCPA	General	Law that grants California consumers data privacy rights and control over personal information.

Security Controls

Tungsten Automation software relies on industry-standard methods to provide security within each application This section includes a general list of compliance controls and methods that you may wish to implement in your business process with Tungsten Automation products.

- Authentication
- Authorization
- Accountability

- Confidentiality/Integrity
- Secure Operational Process
- Security Best Practices

Authentication

Users and services must authenticate with a unique ID as a requirement for accountability. Authentication information is expected to be protected in transit and at rest. Some regulations may require masking of passwords as they are entered. Tungsten Automation Products all leverage Microsoft's Active Directory for authentication.

Note: You can replicate your existing authentication services such as Lightweight Directory Access Protocol (LDAP) into an Active Directory to further leverage existing authentication services.

Authorization

Authorization is how access control is implemented. Based on an authenticated identifier, a user is authorized to perform specific actions in a system. The best practice, Role Based Access Control (RBAC), is simpler to manage than Access Control Lists (ACL), where every object with an ACL must be modified when a user role is changed.

Authorization details must be granular enough to meet the intent of many regulations. In particular, segregation of duties may be required to implement a secure process. This ensures that a single individual cannot manipulate the system to his or her advantage. For example, users who create processes should not also be able to install them. This also means that a product cannot have a single "super" administrator. An additional best practice defines three separate administration role types such as security administration, monitoring administration, and operation administration.

Tungsten Automation Products all implement role-based security and do not require Access Control Lists for authorization. The roles membership is defined as a group or a role configuration object (depending on the specific product involved).

Accountability

Products must support major transaction-level system operations, including create, read, update, and delete (CRUD) auditing. An audit log entry includes at least the following:

- Who (based on unique authorization identifier)
- When
- What operation
- What data/object
- Product used to perform the operation

The log also records authentication attempts where the authentication identity is not known.

Note: To comply with the *EU Privacy Directive 1995/46/EC*, European Union countries operate within limitations on the use of an audit log to monitor employees.

Tungsten Automation Products can log these types of user activities.

Confidentiality / Integrity

Sensitive data in transit (sent over the network) must optionally support integrity (hash) or privacy (encryption) depending on your business requirements. Sensitive data at rest must also be protected. For temporary data, keeping the file open, not allowing sharing, and marking it for deletion is sufficient. For all other cases, encryption must be used.

You can use an Encrypting File System (EFS) to protect data from other users. EFS is not sufficient to protect data if the whole computer is stolen, unless syskey or an external smart card is also used. You can also use whole drive encryption, such as BitLocker, but this does not protect the data from other users. As a best practice, devise an in-depth strategy, store the keys off-machine, and do not tie the key directly to a user account.

Sensitive data often includes personally identifiable information (PII/PHI) and protecting this data is part of HIPAA, PCI DSS and data breach laws. Protecting the integrity of non-sensitive data may also be necessary to prevent out-of-band modification of data that could bypass audit controls implemented on the client side.

Products that directly utilize encryption must support FIPS 140-compliant algorithms when the operating system or application framework runs in FIPS mode. FIPS 140 is required by government agencies with sensitive but unclassified data (SBU), and by some banks.

Longer keys for encryption are not necessarily better. Based on reported vulnerabilities, AES-256 can be weaker than AES-128 in some cases. Choosing an algorithm and key length is a trade-off between speed and length of protection for the data.

Tungsten Automation Products rely on IPsec for in-transit encryption of non-HTTP traffic. SSL and TLS are supported for HTTP traffic. These products additionally all support running with FIPS mode enabled on Windows.

Secure Operational Process

To comply with regulations, your business process may require you to implement IT security processes. The most common requirements include antivirus software, locked-down systems, threat protection, and vulnerability test scans on production systems.

You can use these secure operational processes with Tungsten Automation Products.

Security Best Practices

Tungsten Automation services are designed to run with the least privileges necessary. Tungsten Automation Products validate all their inputs to prevent SQL injection or cross-site scripting attacks in their development process. The latest service pack for the operating system is always supported.

Tungsten Automation Cloud Services offerings are independently audited to the SOC 2 standard for security best practices.

While most security practices generally apply to all Tungsten Automation software, we evaluate each software offering individually, based on the most applicable and appropriate security practices for each product or product class. The evaluation is based on factors including, but not limited to, the target market, product maturity, and target user environment.

Secure Software Development Lifecycle

The Tungsten Automation Secure Software Development Lifecycle (SSDL) helps software development companies reduce the number of security-related design and coding defects, along with the severity of security defects.

The Tungsten Automation SSDL consists of a series of activities designed to address various aspects of security as it relates to the software development process. These activities apply to all phases of the development process, from Planning, Design and Implementation, through Quality Assurance, Release, and Maintenance.

Security Training

Tungsten Automation R&D team members undergo mandatory security training to ensure the resilience of our products, including:

- **Security Awareness Training:** All developers, quality assurance engineers, and product managers within the Tungsten Automation R&D organization are required to complete an annual Security Awareness training course.
- **Security Architects Training:** Security architects within the Tungsten Automation R&D organization are required to complete an annual security training course.
- **Threat Modeling Training:** Security architects and Security Test Leads within the Tungsten Automation R&D organization are required to complete threat modeling training**.**

Security Requirements and Design Assessment

Tungsten Automation R&D performs the following:

- **OWASP ASVS Level 2 Assessment:** Products are assessed against the latest version of the OWASP Application Security and Verification Standard. Products are assessed to reach Security Level 2.
- **Threat Modeling:** Threat modeling exercises are performed on each release for product enhancements that change the security posture of the product.

Implementation

Tungsten Automation R&D performs the following:

- **Static Application Security Testing:** Products are subject to static scans during the development process and for each release. Products are scanned for flaws using industry-standard tools.
- **Software Composition Analysis Scans:** Products are subject to third-party library scans during the development process and for each release. Products are scanned for flaws using the Mend tool.

Verification

Tungsten Automation R&D performs the following testing, as applicable:

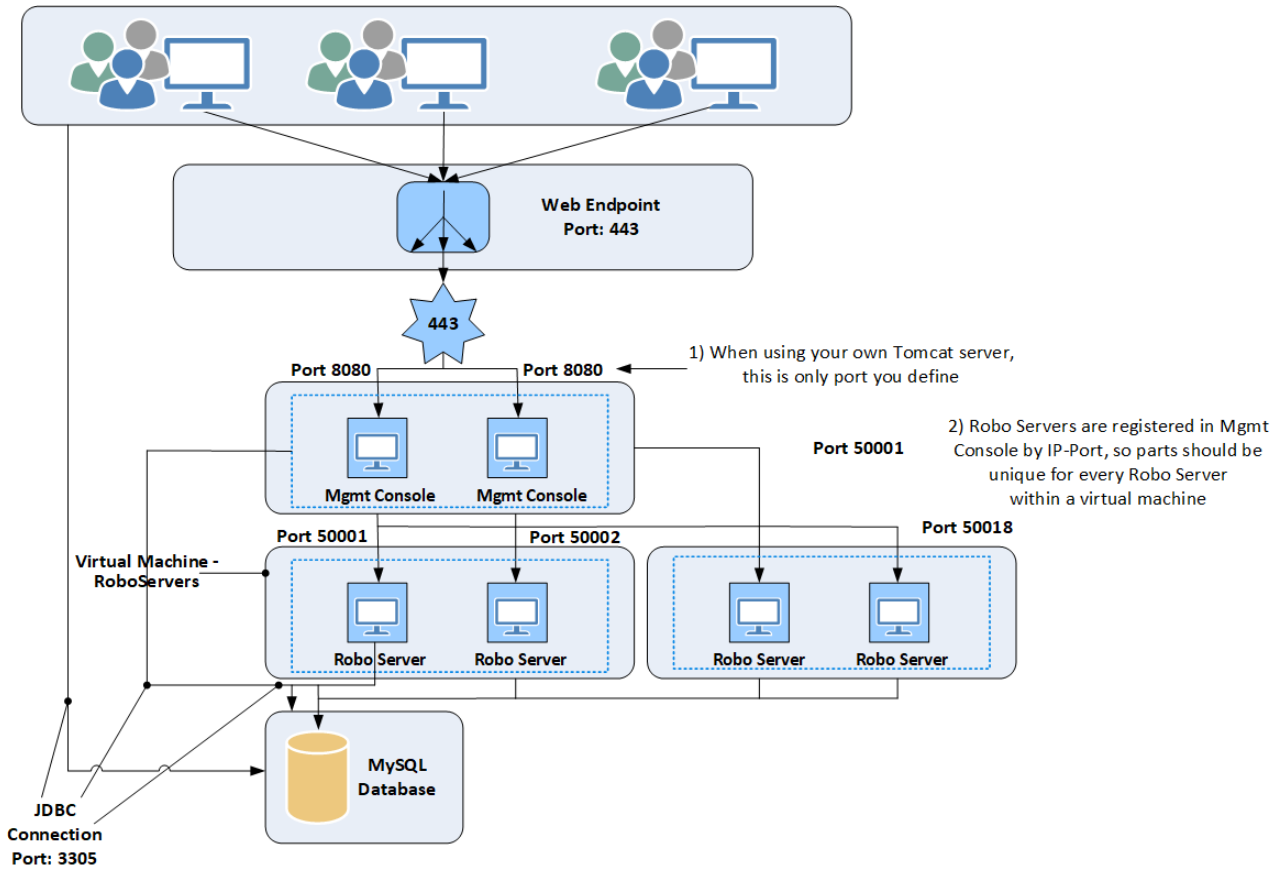
- **Dynamic Application Security Testing**: Products are subject to web vulnerability scans during the development process and for each release. Products are scanned for flaws using industry-standard tools.

Release

- **Independent Penetration Testing:** Qualified products undergo annual penetration testing by an independent firm that specializes in software penetration testing.

Tungsten Automation Security Model Guidelines

Tungsten RPA



A. User login and authentication

Category	Authentication and Authorization
Description	User provides login credentials for the application.
Security Details	Tungsten RPA supports synchronizing users/groups with Active Directory/LDAP. This allows Tungsten RPA to take advantage of the corporate infrastructure for authentication and credential management. Tungsten RPA also has an application-specific authentication and authorization mechanism for convenience. This includes credential management and storage. Stored passwords are encrypted.

B. Client transmits to Tungsten RPA server(s)

Category	Data in transit
Port	80 or 443
Protocol	HTTP or HTTPS
Description	Clients transmit to the Tungsten RPA servers.
Security Details	All connectivity from Tungsten RPA clients (Management Console and Design Studio) to the Tungsten RPA servers is via HTTP/HTTPS. HTTPS should be configured for maximum security.

C. Tungsten RPA server(s) transmits to another Tungsten RPA server(s)

Category	Data in transit
Port	Configurable. Defaults 80, 443, 50000, 50443, 49999, 49998
Protocol	HTTP/HTTPS, socket TCP/IP
Description	Tungsten RPA servers transmit to/from another Tungsten Automation application or server.
Security Details	All Tungsten RPA components can be configured to use secure encrypted communication (TLS 1.2) with custom certificates.

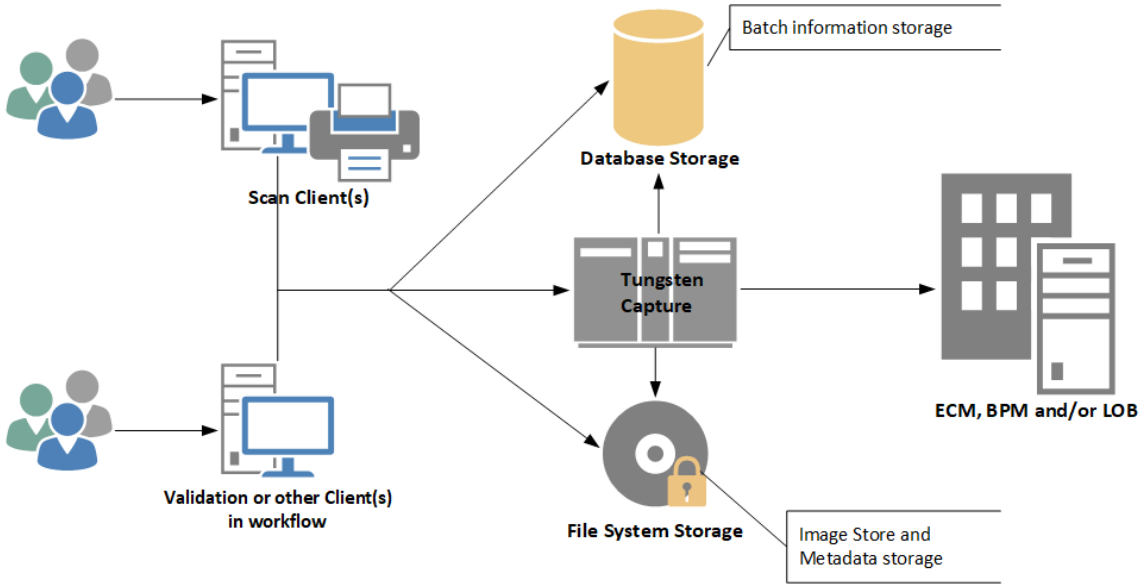
D. Tungsten RPA servers transmit to Database server

Category	Data in transit
Port	Varies depending on protocol
Protocol	TCP/IP
Description	Tungsten RPA servers transmit to/from database
Security Details	The Tungsten RPA servers connect to the SQL database. Typically, the database server system is co-located or otherwise physically protected such that transmission need not be otherwise encrypted. However, if such encryption is needed, you can encrypt the database connection via SSL.

E. Robot and Data storage

Category	Data at rest
Description	Robots, configurations and related metadata are stored via the Management Console. Robots can store customer data in databases.
Security Details	Robots, configurations and related metadata are stored in the Tungsten Automation database, which is accessed through a configured system account. Database level encryption is also available using the encryption feature within the database itself. Whether or not file system and/or database encryption is enabled, passwords (for external systems or application-specific users), are further protected. Passwords stored in the Password Store or as input to a schedule are encrypted using a customer generated certificate. We will use the cipher selected for the certificate to encrypt any stored passwords. By default the installation comes with an RSA 1024 bit encrypted certificate, but we strongly recommend that the customer generates their own certificate.

Tungsten Capture and Tungsten Transformation[1]



A. User login and authentication

Category	Authentication and Authorization
Description	User provides login credentials for the Tungsten Automation application.
Security Details	Tungsten Automation supports corporate directory systems, such as Active Directory through the **Linked Users** and **Linked Groups** features, which take advantage of the corporate infrastructure for authentication and credential management. Tungsten Automation also has an application-specific authentication and authorization mechanism for convenience. This includes credential management and storage. Stored passwords are encrypted. The **Linked Users** feature must be used to take advantage of external systems that provide AES or equivalent encryption.

B. Client transmission to servers

Category	Data in transit
Description	Clients (such as Scan or Validation) transmit to servers.
Communication	Database, .NET Remoting, SMB
Security Details	All streams of data in transit can be protected with IPsec to take advantage of network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. Details on the streams used are as follows: Database information containing metadata is transferred to and from the database using the database manufacturer's client driver. The

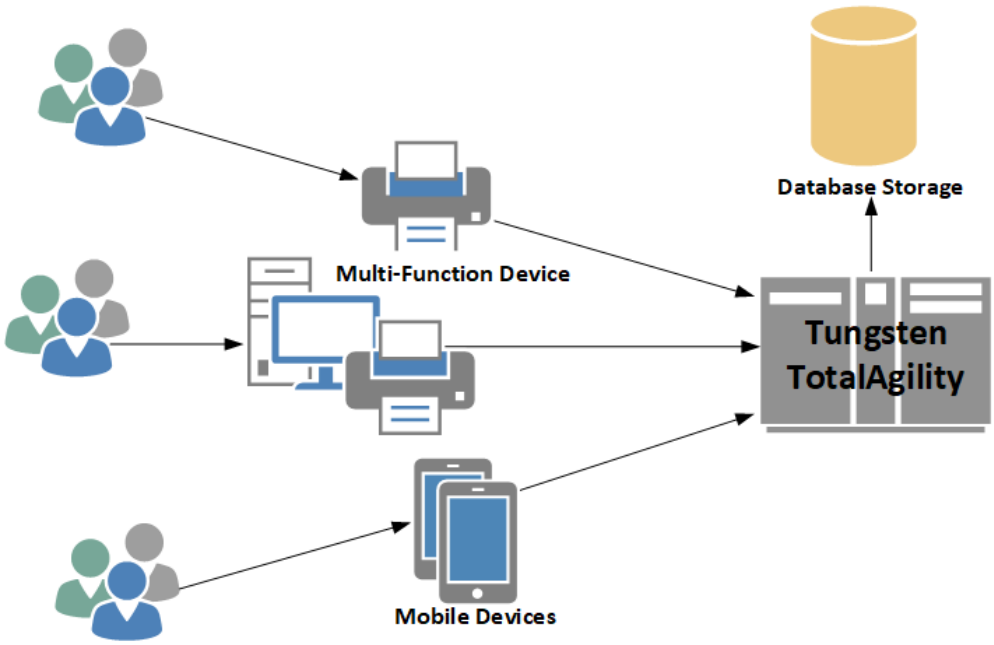
[1] Tungsten Transformation uses the Tungsten Capture security model.

	network protocol varies depending on what database is being used. For more information, consult documentation from your database manufacturer. .NET Remoting (TCP 2424) is used for licensing and batch notification traffic. No confidential information (nothing related to images or metadata) is transmitted or accessed. Images are transmitted to/from the file system using the SMB (TCP 445) protocol.

C. Image and metadata storage

Category	Data at rest
Description	Image and metadata is stored.
Security Details	Images are stored in the file system and can be secured through use of Windows file system permissions. As additional protection, the Tungsten Automation environment should be configured with the SecurityBoost feature that prevents user accounts from accessing the file system outside the application. Images can be also optionally be encrypted via Microsoft BitLocker or Microsoft Encrypting File System (EFS). Metadata is stored in the Tungsten Automation database, which is accessed through a configured system account, or by assigning permissions to each user. Database level encryption is also available by using the encryption feature within the database itself. **Note:** When using Microsoft SQL Server, you must set the "Store batches in SQL Server" configuration option to ensure all metadata is stored in the database. Oracle or IBM DB2 do not offer a comparable option, as all metadata is always stored in the database. Whether or not file system and/or database encryption is enabled, passwords (for external systems or application-specific users), are further protected. Passwords are always stored using the AES encryption algorithm and the SHA2 hashing algorithms approved by the Federal Information Processing Standard (FIPS) Publication 140-2 standard.

Tungsten TotalAgility



A. User login and authentication

Category	Authentication and Authorization
Description	User provides login credentials for Tungsten Automation application.
Security Details	Tungsten Automation supports synchronizing users/groups with Active Directory. This allows Tungsten TotalAgility to take advantage of the corporate infrastructure for authentication and credential management. Tungsten Automation also has an application-specific authentication and authorization mechanism for convenience. This includes credential management and storage. Stored passwords are encrypted. However, because passwords are maintained outside of Tungsten TotalAgility, the users/groups synchronized with Active Directory must be used to take advantage of external systems that provide AES or equivalent encryption. **Note:** Currently, the functionality identified above is only available on-premise.

B. Client transmits to Tungsten TotalAgility server(s)

Category	Data in transit
Port	80 or 443
Protocol	HTTP or HTTPS
Description	Clients transmit to the Tungsten TotalAgility servers.
Security Details	All connectivity from Tungsten TotalAgility clients (including Process/Form Designer, Forms Workspace, Transformation Designer, and MFPs) to the TotalAgility servers is via HTTP/HTTPS. HTTPS should be configured for maximum security.

C. Tungsten TotalAgility server(s) transmits to another Tungsten TotalAgility server(s)

Category	Data in transit
Port	80, 443 or 9001
Protocol	HTTP, HTTPS, WCF NET.TCP
Description	Tungsten TotalAgility servers transmit to/from another Tungsten TotalAgility server. From the TotalAgility web server to an app server or TotalAgility Link Server, HTTP is used by default on port 80. You can also configure HTTPS on port 443. From the TotalAgility app server to a Transformation Server, WCF .NET TCP is used by default on port 9001.
Security Details	All Tungsten TotalAgility components can be deployed on a single machine, in which case there is relatively low risk of a third party intercepting transmission. You can alternately deploy Tungsten TotalAgility components on multiple servers. In such a case, the servers should be co-located and/or physically protected, to mitigate the risk of interception. If further mitigation is desired, use IPsec to protect the connection between machines.

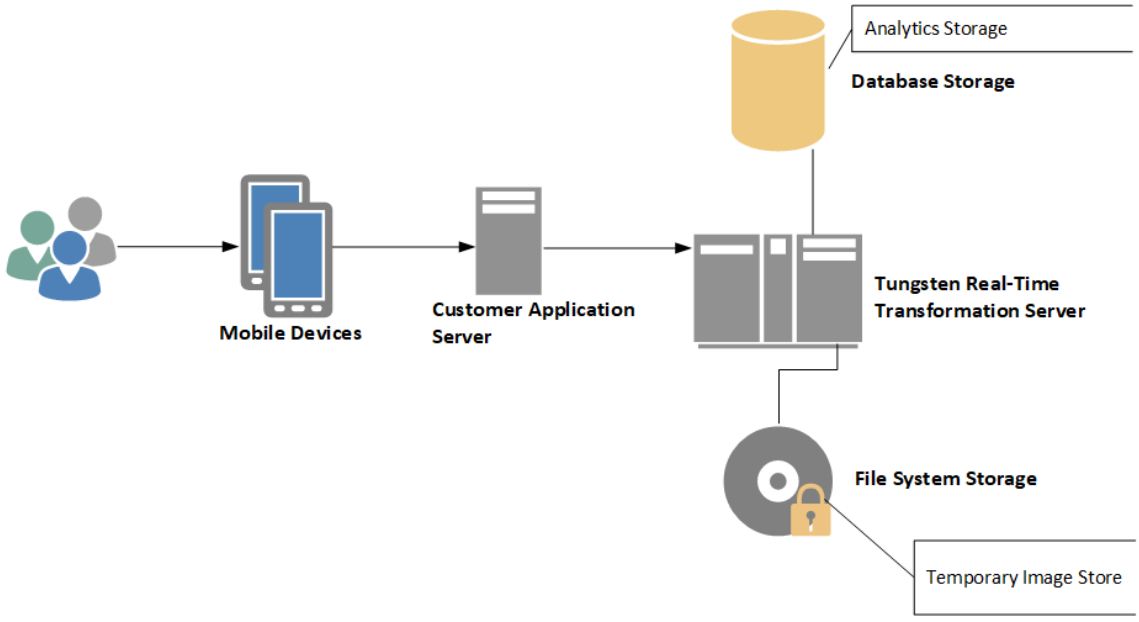
D. Tungsten TotalAgility servers transmit to SQL server

Category	Data in transit
Port	Varies depending on protocol
Protocol	TCP/IP or Named Pipes
Description	Tungsten TotalAgility servers transmit to/from database
Security Details	The Tungsten TotalAgility servers connect to the SQL database. Typically, the SQL Server system is co-located or otherwise physically protected such that transmission need not be otherwise encrypted. However, if such encryption is needed, you can encrypt the database connection via TLS.

E. Image and metadata storage

Category	Data at rest
Description	Image and metadata is stored.
Security Details	Images and metadata are stored in the Tungsten Automation database, which is accessed through a configured system account. Database level encryption is also available using the encryption feature within the database itself. Whether or not file system and/or database encryption is enabled, passwords (for external systems or application-specific users), are further protected. Passwords are always stored using the Triple DES encryption algorithm and the SHA1 hashing algorithms approved by the Federal Information Processing Standard (FIPS) Publication 140-2 standard.

Tungsten Mobile and Real-Time Transformation



A. User login and authentication

Category	Authentication and Authorization
Description	User provides login credentials for Tungsten Automation application or customer Web application.
Security Details	Tungsten Automation supports corporate authentication mechanisms, including Windows authentication. When using a Customer Web Application as middleware between the mobile client and the Tungsten Real-Time Transformation Server, the customer web application handles authentication using a preferred mechanism.

B. Client transmits to Customer Web Application or Tungsten Real-Time Transformation Server

Category	Data in transit
Port	80 or 443
Protocol	HTTP or HTTPS
Description	Client transmits to Customer Web Application or Tungsten Real-Time Transformation Servers.
Security Details	All connectivity from mobile clients to Tungsten Real-Time Transformation Servers use HTTP/HTTPS. Configure HTTPS for maximum security. For maximum security, use HTTPS to configure Customer Web Applications for maximum security.

C. Tungsten Real-Time Transformation Server transmits to SQL Server

Category	Data in transit
Port	Varies depending on protocol

Protocol	TCP/IP or Named Pipes
Description	Tungsten Real-Time Transformation server transmits to/from database
Security Details	The Tungsten Real-Time Transformation Server can optionally connect to a SQL Server database to store analytics information. The SQL Server system is typically co-located or otherwise physically protected eliminating the need for additional encryption. If encryption is required, encrypt the database connection using SSL /TLS protocols.

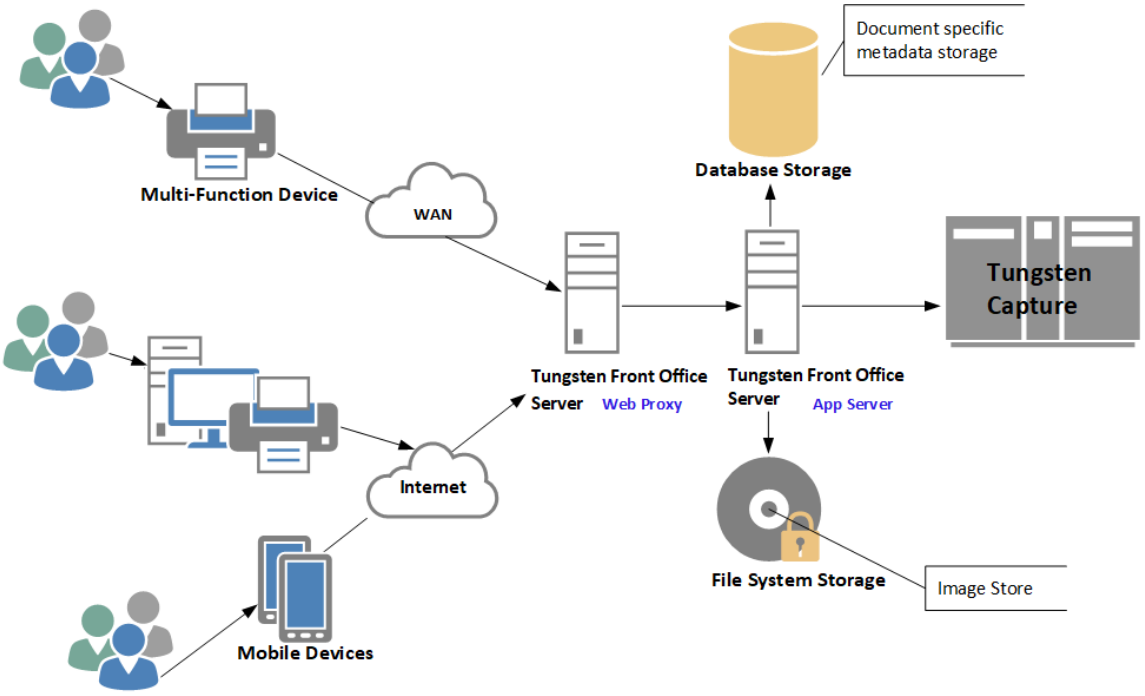
D. Analytics data storage

Category	Data at rest
Description	Analytics data is stored
Security Details	Analytics data is optionally stored in a customer database. Access this database using connection information stored in the web.config file for the Tungsten Real-Time Transformation Server. Use ASP.NET encryption to encrypt associated connection information in the web.config file. When connecting to the database, use Windows authentication for maximum security. Use SQL Server Transparent Data Encryption (TDE) for data at rest.

E. Temporary image storage

Category	Data at rest
Description	Images are stored.
Security Details	Images are stored temporarily for processing. The image storage location is configurable in the web.config file. Use Windows file security controls to restrict folder access to the account running IIS application pool. Use Windows file system encryption for maximum security.

Tungsten Front Office Server



A. User login and **authentication**

Category	Authentication and Authorization
Description	User provides login credentials for the Tungsten Automation application.
Security Details	Tungsten Automation supports corporate authentication systems, such as Active Directory through the Linked Users and Linked Groups features, which take advantage of the corporate infrastructure for authentication and credential management. Tungsten Automation also has an application-specific authentication and authorization mechanism for convenience. This includes credential management and storage. Stored passwords are encrypted. The Linked Users feature must be used to take advantage of external systems that provide AES or equivalent encryption.

B. Multi-Function Device or Web Client connection to Tungsten Front Office Server

Category	Data in transit
Port	80 or 443
Protocol	HTTP or HTTPS
Description	Metadata, including any pre-indexed fields and the images created by the MFP or Thin Client, are sent across the corporate WAN to the Tungsten Front Office Server (web server). Any temporary caching of images and/or index data by the MFP device or browser prior to submission to the KFS server is outside the control of Tungsten Front Office Server.
Security Details	The MFP and web browser traffic can be configured to transmit data securely using SSL/TLS.

C. Connection between Tungsten Front Office Server web server and application

Category	Data in transit
Port	80 or 433
Protocol	HTTP or HTTPS
Description	Metadata, including any pre-indexed fields and the images received at the web server, are transferred to the application server.
Security Details	Metadata can be configured to transmit data securely over SSL/TLS.

D. Tungsten Front Office Server image store

Category	Data at rest
Description	Images created by the MFP are stored briefly for any applicable image cleanup routines or pre-indexing with web client.
Security Details	All images are encrypted by default.

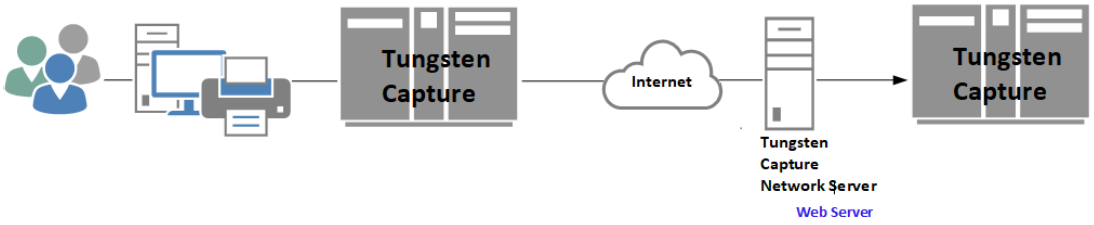
E. Tungsten Front Office Server document-specific data storage

Category	Data at rest
Description	Document-related content is stored in the database, including auditable content (for example, creation date) as well as any pre-indexed information (index fields).
Security Details	The database is password-protected. Further database security is provided by securing access to the machine through standard practices.

F. Metadata and Images sent to Tungsten Capture

Category	Data in transit
Description	Batch is created within Tungsten Capture for back-office processing.
Security Details	Tungsten Front Office Server imports content into Tungsten Capture through a binary interface. The images and index data are stored on the file system. In this context, Tungsten Front Office Server acts as a “client” to Capture (see “Tungsten Capture and Tungsten Transformation” section above). Compared to interactive clients, Tungsten Front Office Server is typically deployed in a protected server room near the Tungsten Capture server, and thus there is relatively low risk of data being intercepted. However, if desired, the Tungsten Front Office Server connection to Tungsten Capture can be further secured.

Tungsten Capture Network Server



A. User login and authentication

Category	Authentication and Authorization
Description	User provides login credentials for the application.
Security Details	Tungsten Automation supports corporate authentication systems, such as Active Directory through the Linked Users and Linked Groups features, which take advantage of the corporate infrastructure for authentication and credential management. Tungsten Automation also has an application-specific authentication and authorization mechanism for convenience. This mechanism includes credential management and storage. Stored passwords are encrypted. The Linked Users feature must be used to take advantage of external systems providing AES or equivalent encryption.

B. Remote Site connection to Tungsten Capture Network Server web server

Category	Data in transit
Port	80 or 443
Protocol	HTTP or HTTPS
Communication	.NET remote method calls
Description	Tungsten Capture can be configured to use SSL to enable security for communications over networks such as the Internet. This allows end-to-end encryption of the Transport Layer.
Security Details	Remote site requests include HTTP GET requests for data from the File Cache and KCN Service, HTTP POSTs to upload files to the File Cache, and .NET remote method calls to the KCN Service.

C. Tungsten Capture Network Server web server connection to the Tungsten Capture Server application server.

Category	Data in transit
Port	2424
Protocol	TCP
Communication	.NET remote method calls
Description	The KCNS Web Server implements a .NET remote method interface that allows remote sites to interact with central site Tungsten Capture system.
Security Details	In this context, Tungsten Capture Network Server acts as a “client” to Tungsten Capture (see Tungsten Capture and Tungsten Transformation.). Compared to interactive clients, Tungsten Capture Network Server is typically deployed in a protected server room near the Tungsten Capture server, and thus with relatively low risk of data being intercepted. If desired, the Tungsten Capture Network Server connection to Tungsten Capture can be further secured as described earlier.

Auditing and Reporting

Tungsten Automation has several features and add-on products that can be used for auditing and reporting purposes. The recommended add-ons for this purpose are Tungsten Analytics for Capture, or Tungsten Analytics for TotalAgility, both of which include a broad set of auditing data and advanced dynamic dashboards for data analysis.

Tungsten RPA can be configured to provide audit log information using Log4J logging to direct log messages to the preferred logging or auditing system. In addition to the standard system logging for monitoring, it is also possible to enable logging of all http(s) requests performed by the system, to verify that there is no access to unauthorized data sources.

Tungsten Capture customers with minimal auditing and reporting requirements may also consider the Tungsten Capture Report Viewer, which includes five standard reports. The Tungsten Capture User Tracking feature must be enabled to collect the statistical data for these reports.

Tungsten Automation Products additionally include extensibility using scripting. Customers can add custom scripts to address any custom auditing needs that may arise.

Refer to the product documentation for more details.

Login Audits

Auditing login behavior is key to many security policies because it allows you to understand who is doing what in the system, and when. Additionally, it is important to know about failed login attempts to determine whether someone is attempting to break into a specific account. Auditing login behavior is best accomplished using Windows audit logging.

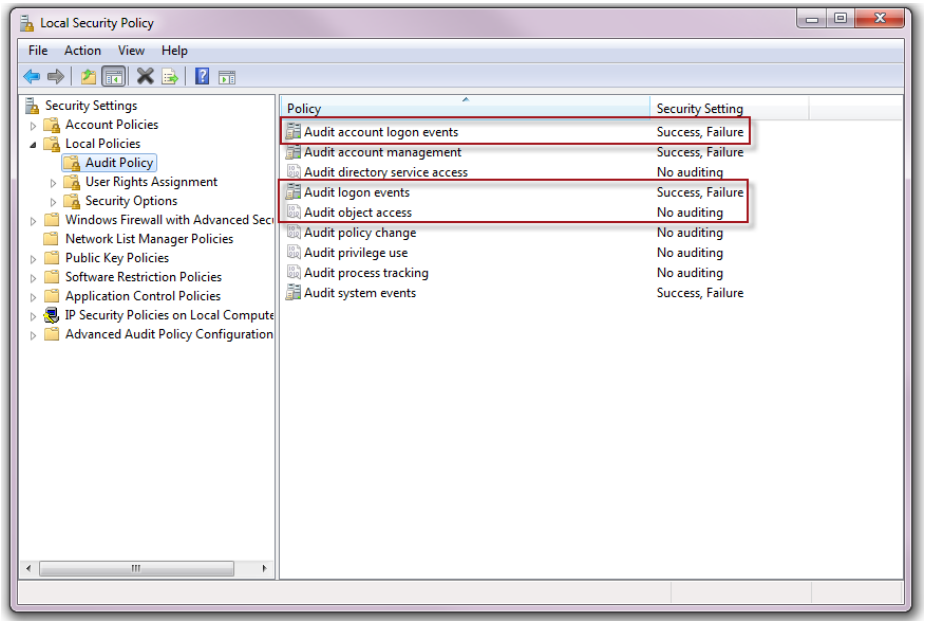
The following steps assume the Tungsten Automation administrator has linked or synchronized domain user accounts and authentication to Active Directory to utilize SSO. You can modify the steps according to your business requirements.

Note: You must enable Windows audit logging to track login success and failure, along with Tungsten Automation module access in the operating system on each station where Tungsten Automation Products are run.

Enable Audit login in **Local Security Settings > Local Policies > Audit Policy** on each machine that will run Tungsten Automation Products.

1. Enable **Success** and **Failure** for at least the following Policies:
    - Audit account login events
    - Audit login events
    - Audit object access

You can enable additional policies as needed.



Note: You can additionally enable Windows auditing on the specific Tungsten Automation thick client applications.

2. Locate the executable for the specific application.
3. Right-click the application (.exe) and select **Properties**.
4. On the Security window, click **Advanced**.
5. On the Auditing window, click **Add**.
6. In the Auditing Entry > Objects window, select the level of **Successful** and **Failed** access for a user.
7. Enter **Everyone** in the name field to define access rights for all users.

After you configure auditing for the machine and required applications, you can view Security Audits in the machine **Security** option, **Event Viewer**.

Login Timeouts

To prevent unauthorized access to unattended systems, we recommend that you configure a timeout after inactivity.

For Tungsten Automation thick-client modules, Tungsten Automation recommends implementation of Windows-based session timeouts or Citrix-based application timeouts depending on the specific use case and environment. Citrix should be utilized such that the application opens directly rather than a desktop-based session. This allows Citrix to close down the application when the configured session times out.

For Tungsten Automation thin client modules, Tungsten Automation supports an application-level timeout. Consult the product documentation for more details.

Payment Card Industry Data Security Standard

Tungsten Automation Platform and PCI DSS

The PCI DSS (Payment Card Industry Data Security Standard) security standard requirements cover a broad spectrum of security disciplines including security management, policies, procedures, network architecture, software design and other critical protective measures. You configure Tungsten Automation software using external processing environments to meet PCI DSS compliance.

A Tungsten Automation solution captures unstructured data in paper and a variety of other formats, classifying and validating that data before transforming the data into actionable information for additional processing. The Tungsten Automation solution is not a data repository and does not maintain or store exported data. The information in this section describes PCI DSS compliance in this operating context.

Tungsten Automation software uses a Microsoft Windows environment to leverage the underlying functionality of the Windows operating system for base security facilities. For example, Tungsten Automation Software uses Active Directory for SSO and is certified to operate with Microsoft IPsec and EFS subsystems.

- Data in transit
- Data at rest
- Controlling access to data

These concepts are covered in the Tungsten Automation Security Model section in this document.

Tungsten Automation Platform and PCI DSS Requirements

Compliance

The PCI DSS requirements are broad and wide ranging. While a number of the requirements involve technology solutions that are addressed directly by the Tungsten Automation platform and the underlying operating system, some require measures external to the Tungsten Automation platform to ensure compliance. The following table shows how the Tungsten Automation platform facilitates, contributes, and requires external measures to meet each requirement.

Facilitated by Tungsten Automation platform and Windows operating system
Requires external measures (includes procedural requirements)
Partially facilitated by features in Tungsten Automation platform and Windows operating system

Requirement	Sub-requirements									
1. Install and maintain a firewall configuration to protect cardholder data	1.1	1.2	1.3	1.4	1.5					
2. Do not use vendor-supplied defaults for system passwords and other security parameters	2.1	2.2	2.3	2.4	2.5	2.6				
3. Protect stored cardholder data	3.1	3.2	3.3	3.4	3.5	3.6	3.7			
4. Encrypt transmission of cardholder data across open, public networks	4.1	4.2	4.3							
5. Use and regularly update antivirus software or programs	5.1	5.2	5.3	5.4						
6. Develop and maintain secure systems and applications	6.1	6.2	6.3	6.4	6.5	6.6	6.7			
7. Restrict access to cardholder data by business need to know	7.1	7.2	7.3							
8. Assign a unique ID to each person with system component access	8.1	8.2	8.3	8.4	8.5	8.6	8.7	8.8		
9. Restrict physical access to cardholder data	9.1	9.2	9.3	9.4	9.5	9.6	9.7	9.8	9.9	9.10
10. Track and monitor all access to network resources and cardholder data	10.1	10.2	10.3	10.4	10.5	10.6	10.7	10.8		
11. Regularly test security systems and processes	11.1	11.2	11.3	11.4	11.5	11.6				
12. Maintain a policy that addresses information security for all personnel	12.1	12.2	12.3	12.4	12.5	12.6	12.7	12.8	12.9	12.10

Note: The cloud services used by Tungsten Clarity have been reviewed by an independent Qualified Security Accessor and are determined to be PCI DSS 3.2.1 compliant.

Objective 1: Build and Maintain Security Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirement 1	Tungsten Automation Platform
1.1 Establish firewall and router configuration standards.	Process and procedure, requires measures external to the Tungsten Automation platform.
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	Process and procedure, requires measures external to the Tungsten Automation platform.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Process and procedure, requires measures external to the Tungsten Automation platform.
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	Process and procedure, requires measures external to the Tungsten Automation platform.
1.5 Document firewall management security polices and operational procedures and ensure they are in use and known to all affected parties.	Process and procedure, requires measures external to the Tungsten Automation platform.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirement 2	Tungsten Automation platform
2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	Process and procedure, requires measures external to the Tungsten Automation platform.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Process and procedure, requires measures external to the Tungsten Automation platform.
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	The Tungsten Automation platform is certified to operate with IPsec, and HTTPS.
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data.	Process and procedure, requires measures external to the Tungsten Automation platform.
2.5 Document management of vendor default security polices and operational procedures and other security parameters, and ensure these are known to all affected parties, and in use.	Process and procedure, requires measures external to the Tungsten Automation platform.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in the Payment Card Industry (PCI) Data Security Standard document.[2]	Process and procedure, requires measures external to the Tungsten Automation platform.

[2] https://www.pcisecuritystandards.org

Objective 2: Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Requirement 3	Tungsten Automation platform
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	The Tungsten Automation platform only stores data temporarily during processing and does not need to retain any data post processing.
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	The Tungsten Automation platform does not process card chip data or magnetic strip data other sensitive data such as PINs, PIN blocks, or CVV2, held on paper that may be scanned in as part of processing and can be redacted.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Some Tungsten Automation products support redaction (blacking out) of sensitive information held on an image. Please see product-specific documentation for details.
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures	Supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on the mix of Tungsten Automation Products used.
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.	Process and procedure, requires measures external to the Tungsten Automation platform.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	Process and procedure, requires measures external to the Tungsten Automation platform.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Process and procedure, requires measures external to the Tungsten Automation platform.

Requirement 4: Encrypt transmission of cardholder data across open public networks

PCI DSS Requirement 4	Tungsten Automation platform
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPsec to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in the scope of the PCI DSS include: ▪ The Internet ▪ Wireless technologies ▪ Global System for Mobile communications (GSM) and	Supports the use of Windows IPsec and HTTPS.

PCI DSS Requirement 4	Tungsten Automation platform
General Packet Radio Service (GPRS)	
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, email, instant messaging, or chat).	Standard processing does not require use of messaging technologies.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Process and procedure, requires measures external to the Tungsten Automation platform.

Objective 3: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update antivirus software or programs

PCI DSS Requirement 5	Tungsten Automation platform
5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Process and procedure, requires measures external to the Tungsten Automation platform.
5.2 Ensure that all antivirus mechanisms are current, actively running, and capable of generating audit logs.	Process and procedure, requires measures external to the Tungsten Automation platform.
5.3 Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Process and procedure, requires measures external to the Tungsten Automation platform.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Process and procedure, requires measures external to the Tungsten Automation platform.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirement 6	Tungsten Automation platform
6.1 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	Process and procedure, requires measures external to the Tungsten Automation platform.
6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	Process, requires measures external to the Tungsten Automation platform.
6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout software development.	For components developed as part of an implementation process and Procedure, requires measures external to the Tungsten Automation platform.
6.4 Follow change control procedures for all changes to system components.	Process and procedures, requires measures external to the Tungsten Automation platform.

PCI DSS Requirement 6	Tungsten Automation platform
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development	For components developed as part of an implementation process and procedure, requires measures external to the Tungsten Automation platform.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: ▪ Reviewing public-facing web applications with manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications	Process and procedures, requires measures external to the Tungsten Automation platform.
6.7 Document security policies and operational procedures for developing and maintaining secure systems and applications. Ensure these policies and procedures are in use and are known to all affected parties.	Process and procedures, requires measures external to the Tungsten Automation platform.

Objective 4: Implement String Access Control Maintenance

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Requirement 7	Tungsten Automation platform
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system.
7.2 Establish an access control system for system components with multiple users that restricts access based on a user's need to know, and is set to **deny all** unless specifically allowed.	Supported by profiles in the Tungsten Automation platform and policies within the Windows operating system.
7.3 Document security policies and operational procedures for restricting access to cardholder data. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedures, requires measures external to the Tungsten Automation platform.

Requirement 8: Assign a unique ID to each person with system component access

PCI DSS Requirement 8	Tungsten Automation platform
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Supported by Tungsten Automation platform.

PCI DSS Requirement 8	Tungsten Automation platform
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Password or passphrase • Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	Supported by Tungsten Automation platform in conjunction with Windows operating system.
8.3 Incorporate two-factor authentication for remote network access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	Supported by Windows operating system.
8.4 Document and communicate authentication procedures and policies to all users.	Process and procedure requires measures external to the Tungsten Automation platform.
8.5 Do not use group, shared, or generic IDs, passwords or other authentication methods to administer any system components.	Process and procedure, requires measures external to the Tungsten Automation platform.
8.6 Where other authentication mechanisms are used, such as physical or logical security tokens, smart cards, or certificates, use of these mechanisms must be assigned as follows: • To an individual account not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Process and procedure, requires measures external to the Tungsten Automation platform.
8.7 Restrict access to any database containing cardholder data (including access to applications, administrators, and all other users) including the following: • User access to databases through programmatic methods. • Only database administrators can directly access or query databases. • Only applications can use application IDs for databases.	Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system.
8.8 Document security policies and operational procedures for identification and authentication. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure requires measures external to the Tungsten Automation platform.

Requirement 9: Restrict physical access to cardholder data

PCI DSS Requirement 9	Tungsten Automation platform
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Requires measures external to the Tungsten Automation platform.
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. For purposes of this requirement, **employee** refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are **resident** on the entity's site. A **visitor** is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.	Process and procedure, requires measures external to the Tungsten Automation platform.
9.3 Make sure all visitors are handled correctly.	Process and procedure, requires measures external to the Tungsten Automation platform.
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Process and procedure requires measures external to the Tungsten Automation platform.
9.5 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Process and procedure, requires measures external to the Tungsten Automation platform.
9.6 Physically secure all paper and electronic media that contain cardholder data.	Process and procedure, requires measures external to the Tungsten Automation platform.
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.	Process and procedure, requires measures external to the Tungsten Automation platform.
9.8 Destroy media containing cardholder data when it is no longer needed for business or legal reasons.	Tungsten Automation platform can remove post processed images containing cardholder data. Process and procedure requires measures external to the Tungsten Automation platform to comply generally.
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	Process and procedure requires measures external to the Tungsten Automation platform.
9.10 Document security policies and operational procedures for restricting physical access to cardholder data. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure requires measures external to the Tungsten Automation platform.

Objective 5: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Requirement 10	Tungsten Automation platform
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	Achieve by defining group policies in Windows operating system and Tungsten Automation profiles.
10.1 Implement automated audit trails for all system components.	The Tungsten Automation platform can contribute to this requirement but requires measures external to the Tungsten Automation platform to fully conform.
10.3 Record audit trail entries for all system components for each event	The Tungsten Automation platform can record the required information for its components.
10.4 Synchronize all critical system clocks and times.	Process and procedure, requires measures external to the Tungsten Automation platform.
10.5 Secure audit trails so they cannot be altered.	The Tungsten Automation platform can contribute to this requirement but requires measures external to the Tungsten Automation platform to fully conform.
10.6 Review logs for all system components at least daily. Log reviews must include servers that perform security functions such as intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).	Process and procedure, requires measures external to the Tungsten Automation platform.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Process and procedure, requires measures external to the Tungsten Automation platform.
10.8 Document security policies and operational procedures for monitoring all access to network resources and cardholder data. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure, requires measures external to the Tungsten Automation platform.

Requirement 11: Regularly test security systems and processes

PCI DSS Requirement 11	Tungsten Automation platform
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	Process and procedure, requires measures external to the Tungsten Automation platform.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.	Process and procedure, requires measures external to the Tungsten Automation platform.
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification.	Process and procedure, requires measures external to the Tungsten Automation platform.

PCI DSS Requirement 11	Tungsten Automation platform
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	Process and procedure, requires measures external to the Tungsten Automation platform.
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Process and procedure, requires measures external to the Tungsten Automation platform.
11.6 Document security policies and operational procedures for security monitoring and testing. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure, requires measures external to the Tungsten Automation platform.

Objective 6: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Requirement 12	Tungsten Automation platform
12.1 Establish, publish, maintain, and disseminate a security policy.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.2 Implement a risk assessment process that identifies assets, threats, vulnerabilities, and results and ensure the process is performed at least annually.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.5 Assign information security management responsibilities to an individual or team.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.7 Screen potential employees (see definition of **employee** at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	Process and procedure, requires measures external to the Tungsten Automation platform.

PCI DSS Requirement 12	Tungsten Automation platform
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.9 Establish a best practice for written acknowledgement of service provider responsibility for the security of cardholder data. **Note:** As of June 30, 2015, this practice is a requirement.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	Process and procedure, requires measures external to the Tungsten Automation platform.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule defines United States national standards protecting electronic personal health information stored by health care providers. HIPAA also requires appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and security of electronic protected health information.

The HIPAA Privacy Rule defines additional privacy standards protecting medical records and other personal health information. The rule requires safeguards to protect patient information sharing without the consent of the patient. The rule applies to providers and their representatives.

Note: HIPAA standards do not specify implementation details. Exact steps to meet HIPAA privacy standards are often left up to companies and/or consulting organizations. As many of the HIPAA requirements are similar to those for the Payment Card Industry Data Security Standard (PCI), Tungsten Automation has used PCI requirements as a basis for HIPAA recommendations.

Privacy Rule

The HIPAA Privacy Rule provides standards to protect medical records and other personal health information (PHI) and sets limits on use and disclosure of this information. The Privacy Rule applies to electronic health information (ePHI), as well as oral and written personal health information. These privacy rules also provide individuals with access and correction request rights to their personal health information.

Security Rule

The HIPAA Security Rule establishes standards to protect electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity. This rule requires sufficient administrative, physical, and technical safeguards to ensure confidentiality, integrity, and security of this information. The Security Rule is more comprehensive than the Privacy Rule, providing detailed requirements specific to ePHI.

Tungsten Automation Products and PHI / HIPAA Compliance

Although the overall IT ramifications of HIPAA are beyond the scope of this document, we believe the following topics are key to our customers to meet HIPAA requirements for Tungsten Automation Products.

- Data in transit
- Data at rest
- Audit logging and reporting
- Session timeout

These concepts are covered in the Tungsten Automation Security Model section of this document.

The Tungsten Automation platform and HIPAA Security and Privacy

The U.S. Department of Health and Human Services and the Secretary of Health and Human Services maintain national standards and HIPAA rule regulations for electronic health care providers, health insurance providers, and other healthcare industry employers.[3]

The following table shows control objectives and associated recommendations. The objectives are divided further into more detailed sub-recommendations with testing procedures, for more in-depth understanding of the security and privacy standards.

Control Objective	Standard
Administrative Safeguards	1. Security Management
	2. Workforce Security
	3. Information Access Management
	4. Workforce Training
	5. Evaluation and Reporting
	6. Contingency Plan
Physical Safeguards	7. Facility Access Controls
	8. Workstations
	9. Device and Media Controls
Technical Safeguards	10. Access Control
	11. Audit Controls
	12. Authentication
	13. Transmission

Administrative Safeguards

- Security measures with careful consideration of risk and risk management required to protect the data integrity, and privacy while providing secure access to protected health information.
- Actions, policies and procedures required to manage and maintain ePHI security, including workforce management and the reliability of secure access to the data by the appropriate workforce.

Physical Safeguards

- Physical measures, policies and procedures to protect electronic information systems from internal and external risks.
- Security measures to protect related buildings and equipment, from natural and environmental hazards, or unauthorized intrusion.

Technical Safeguards

- Technology, policies, and procedures to control access to ePHI.

[3] https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

Tungsten Automation platform and HIPAA Standards

Compliance

HIPAA standards are broad and wide-ranging. While a number of the requirements involve technology solutions that are addressed directly by the Tungsten Automation platform and the underlying operating system, some require measures external to the Tungsten Automation platform to ensure compliance. The following table shows how the Tungsten Automation platform facilitates, contributes, and requires external measures to meet each requirement.

Facilitated by Tungsten Automation platform and Windows operating system
Requires external measures (includes procedural requirements)
Partially facilitated by features in Tungsten Automation platform and Windows operating system

Requirement	Sub-requirements							
Administrative Safeguards								
1. Security Management Processes	1.1	1.2	1.3	1.4				
2. Workforce Security	2.1	2.2	2.3	2.4				
3. Information Access Management	3.1	3.2	3.3					
4. Workforce Training	4.1	4.2	4.3	4.4	4.5			
5. Evaluation and Reporting	5.1	5.2	5.3					
6. Contingency Plan	6.1	6.2	6.3	6.4	6.5			
Physical Safeguards								
7. Facility Access Control	7.1	7.2	7.3	7.4				
8. Workstations	8.1	8.2						
9. Device and Media Controls	9.1	9.2	9.3	9.4				
Technical Safeguards								
10. Access Control	10.1	10.2	10.3	10.4.a	10.4.b	10.4.c	10.4.d	10.4.e
11. Audit Controls	11.1	11.2	11.3					
12. Authentication	12.1	12.2	12.3					
13. Transmission	13.1	13.2						

Objective 1: Administrative Safeguards (§164.308)

Standard 1: Security Management Processes §164.308(a)(1)

Implement policies and procedures to prevent, detect, contain, and correct security violations.

Note: Implementation Specifications are indicated after each HIPAA standard.

- (R) Required

- (A) Addressable

HIPAA Standard	Tungsten Automation platform
1.1 *Risk Management (R)* —§164.308(a)(1)(ii)(A) & (B); §164.306(a) Assess potential risks to the accessibility, privacy, and reliability of ePHI and implement reasonable security measures.	Process and procedure, requires measures external to the Tungsten Automation platform.
1.2 *Sanction Policy (R)* —§164.308(a)(1)(ii)(C) Apply appropriate sanctions against workforce members who fail to comply with security measures.	Process and procedure, requires measures external to the Tungsten Automation platform.
1.3 *Information System Activity Review (R)* — §164.308(a)(1)(ii)(D) Implement regular information system activity review.	Process and procedure, requires measures external to the Tungsten Automation platform.
1.4 *Assigned Security Responsibility (R)* —§164.308(a)(i)(2) Identify individuals responsible for the design and implementation of security management processes.	Process and procedure, requires measures external to the Tungsten Automation platform.

Standard 2: Workforce Security §164.308(a)(3)(i)

Implement policies and procedures to ensure workforce has appropriate access to ePHI.

HIPAA Standard	Tungsten Automation platform
2.1 *Authorization and/or Supervision (A)* —§164.308(a)(3)(i)(A) Define and implement policies and procedures allowing and/or restricting workforce individual's access to ePHI.	Process and procedure requires measures external to the Tungsten Automation platform. **Note**: Tungsten Automation Products have user management that allows restricting access to any information stored by Tungsten Automation.
2.2 *Workforce Clearance Procedure (A)* —§164.308(a)(3)(i)(B) Implement procedures to determine appropriate access of a workforce member to ePHI.	Process and procedure requires measures external to the Tungsten Automation platform.
2.3 *Termination Procedures (A)* —§164.308(a)(3)(i)(C) Implement procedures regarding termination of access rights to ePHI.	Process and procedure requires measures external to the Tungsten Automation platform.
2.4 *Business Associate Contracts and Other Arrangement (A)* —§164.308(b)(1); §164.314(a) Define and implement policies and procedures to allow a business associate access to ePHI with satisfactory assurance the business associate will safeguard the information.	Process and procedure requires measures external to the Tungsten Automation platform.

Standard 3: Information Access Management §164.308(a)(4)(i)

Implement policies and procedures to authorize access to ePHI.

HIPAA Standard	Tungsten Automation platform
3.1 *Isolating Health Care Clearinghouse Function (R)* — §164.308(a)(4)(ii)(A) Implement policies and procedures to protect ePHI managed by a health care clearinghouse from unauthorized access by the larger organization.	Process and procedure, requires measures external to the Tungsten Automation platform.

HIPAA Standard	Tungsten Automation platform
3.2 *Access Authorization (A)* —§164.308(a)(4)(ii)(B) Implement policies and procedures regarding grant of access rights to ePHI.	Process and procedure, requires measures external to the Tungsten Automation platform.
3.3 *Access Establishment and Modification (A)* —§164.308(a)(4)(ii)(C) Implement policies and procedures to document, review, and modify user access to a workstation, transaction, program, or process.	Process and procedure, requires measures external to the Tungsten Automation platform.

Standard 4: Workforce Training §164.308(a)(5)

Implement workforce security awareness training including periodic security reminders, protection from malicious software, log-in monitoring, and password management.

HIPAA Standard	Tungsten Automation platform
4.1 *Standard Security awareness training (A)* —§164.308(a)(5)(i) Implement a security awareness and training program for workforce and management.	Process and procedure, requires measures external to the Tungsten Automation platform.
4.2 *Security Reminders (A)* —§164.308(a)(5)(i)(A) Periodic security updates.	Process and procedure, requires measures external to the Tungsten Automation platform. Tungsten Automation Products issue periodic updates, including security updates.
4.3 *Protection from Malicious Software (A)* —§164.308(a)(5)(i)(B) Procedures to guard against, detect, and report malicious software.	Use and regularly update antivirus software or programs Develop and maintain secure systems and applications
4.4 *Log-in Monitoring (A)* —§164.308(a)(5)(i)(C) Procedures to monitor log-in attempts and to report discrepancies.	Process and procedure, requires measures external to the Tungsten Automation platform. Supported by Tungsten Automation platform in conjunction with Windows operating system. See Login Audits for more information.
4.5 *Password Management (A)* —§164.308(a)(5)(i)(D) Procedures to create, change, and safeguard passwords.	Process and procedure, requires measures external to the Tungsten Automation platform. Supported by Tungsten Automation platform in conjunction with Windows operating system.

Standard 5: Reporting and Evaluation §164.308(a)(6) & §164.308(a)(8)

Implement procedures to evaluate, maintain, and report on established security policies.

HIPAA Standard	Tungsten Automation platform
5.1 *Security Incident Procedures (R)* —§164.308(a)(6)(i) Implement policies and procedures to address security incidents.	Process and procedure, requires measures external to the Tungsten Automation platform.
5.2 *Response and Reporting Procedures(R)* —§164.308(a)(6)(ii) Identify and respond to suspected or known security	Tungsten Automation platform can contribute to this requirement but requires measures external

HIPAA Standard	Tungsten Automation platform
incidents; mitigate, to the extent practicable, harmful effects of known security; and document security incidents and their outcomes.	to the Tungsten Automation platform in order to fully conform. See Auditing and Reporting for additional information.
5.3 *Evaluation (R)* —§164.308(a)(8) In response to environmental or operational changes, perform periodic technical and nontechnical evaluation of ePHI security policies and procedures to determine if they continue to meet requirements.	Process and procedure, requires measures external to the Tungsten Automation platform.

Standard 6: Contingency Plan §164.308(a)(1)

Establish policies to protect ePHI during emergencies such as system failure, fire, vandalism, or natural disaster.

HIPAA Standard	Tungsten Automation platform
6.1 *Data Backup Plan (R)* —§164.308(a)(7)(ii)(A) Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Process and procedure requires measures external to the Tungsten Automation platform.
6.2 *Disaster Recovery Plan (R)* —§164.308(a)(7)(ii)(B) Define procedures to restore any data loss.	Process and procedure requires measures external to the Tungsten Automation platform.
6.3 *Emergency Mode Operation Plan (R)* —§164.308(a)(7)(ii)(C) Define procedures to enable continuation of critical business processes to protect ePHI security while operating in emergency mode.	Process and procedure requires measures external to the Tungsten Automation platform.
6.4 *Testing and Revision Procedure (A)* —§164.308(a)(7)(ii)(D) Implement procedures for periodic tests and revisions of contingency plans.	Process and procedure requires measures external to the Tungsten Automation platform.
6.5 *Applications and Data Criticality Analysis (A)* §164.308(a)(7)(ii)(E)— Implement procedures for periodic contingency plan tests and revisions.	Process and procedure requires measures external to the Tungsten Automation platform.

Objective 2: Physical Safeguards (§164.310)

Limit physical access to electronic information systems and facilities containing ePHI.

Standard 7: Facility Access Controls §164.310(a)(1)

Note: Implementation Specifications are indicated after each HIPAA Standard.

- (R) Required
- (A) Addressable

HIPAA Standard	Tungsten Automation platform
7.1 *Contingency Operations (A)* —§164.310(a)(2)(i) Define a disaster recovery plan to support lost data recovery	Process and procedure, requires measures external to the Tungsten Automation platform.

HIPAA Standard	Tungsten Automation platform
and emergency mode operations.	
7.2 *Facility Security Plan (A)* —§164.310(a)(2)(ii) Implement facility security policies and procedures to safeguard against unauthorized physical access, tampering, and theft.	Process and procedure, requires measures external to the Tungsten Automation platform.
7.3 *Access Control and Validation Procedures (A)* —§164.310(a)(2) (iii) Implement procedures to control and validate facility access, including visitor control and access to software programs for testing and revision.	Process and procedure, requires measures external to the Tungsten Automation platform.
7.4 *Maintenance Records (A)* —§164.310(a)(2) (iv) Implement policies and procedures to document facility repairs and modifications to the physical components of a facility related to security such as doors and locks.	Process and procedure, requires measures external to the Tungsten Automation platform.

Standard 8: Workstation and Device Security §164.310(b) and (c)

HIPAA Standard	Tungsten Automation platform
8.1 *Workstation Use (R)* —§164.310(b) Implement policies and procedures for proper use of workstations that can access ePHI, including the surrounding area.	Process and procedure, requires measures external to the Tungsten Automation platform.
8.2 *Workstation Security (R)* —§164.310(c) Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Process and procedure, requires measures external to the Tungsten Automation platform. Tungsten Automation platform is certified to operate with IPsec and HTTPS.

Standard 9: Device and Media Controls §164.310(d)(1)

Implement policies and procedures to govern receipt, removal, and movement within the facility of hardware and electronic media containing ePHI.

HIPAA Standard	Tungsten Automation platform
9.1 *Disposal (R)* —§164.310(d)(2)(i) Implement policies and procedures for final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Process and procedure, requires measures external to the Tungsten Automation platform.
9.2 *Media Re-use (R)* —§164.310(d)(2)(ii) Implement procedures for removal of ePHI from electronic media.	Process and procedure requires measures external to the Tungsten Automation platform.
9.3 *Accountability (A)* —§164.310(d)(2) (iii) Maintain a record of the movements of hardware and electronic media, including a record of any individual responsible for the movement.	Process and procedure requires measures external to the Tungsten Automation platform.
9.4 *Data Backup and Storage (A)* —§164.310(d)(2) (iv) Create a retrievable, exact ePHI copy, when needed, before movement of equipment.	Process and procedure requires measures external to the Tungsten Automation platform.

Objective 3: Technical Safeguards (§164.312)

Standard 10: Access Control §164.312(a)(1)

Implement technical policies and procedures to maintain electronic information systems containing ePHI.

Note: Implementation Specifications are indicated after each HIPAA Standard.

- (R) Required
- (A) Addressable

HIPAA Standard	Tungsten Automation platform
10.1 *Unique User Identification (R)* —§164.312(a)(2)(i) Assign unique user identity name or number.	Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system.
10.2 *Emergency Access Procedure (R)* —§164.312(a)(2)(ii) Establish procedures to obtain necessary ePHI during an emergency.	Process and procedure requires measures external to the Tungsten Automation platform. Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system.
10.3 *Automatic Logoff (A)* —§164.312(a)(2) (iii) Implement electronic procedures to terminate an electronic session after a predetermined period of inactivity.	Process and procedure requires measures external to the Tungsten Automation platform. Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows Operating System. See Login Timeouts for additional information.
10.4 *Encryption and Decryption (A)* —§164.312(a)(2) (iv) 10.4.a Implement ePHI encryption and decryption method.	Process and procedure, requires measures external to the Tungsten Automation platform.
10.4.b Render personal health information unreadable anywhere it is stored	Supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on mix of Tungsten Automation Products used.
10.4.c Protect personal health data at rest	Tungsten Automation databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. The full level of SQL encryption is supported.
10.4.d Password and server configurations	Tungsten Automation databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. The full level of SQL encryption is supported. **Note:** For data in transit, access within a secure intranet configuration may not require encryption.
10.4.e Encrypt transmission of personal health information across open public networks	Tungsten Automation supports the use of Windows IPsec, HTTPS, or site-to-site VPN.

Standard 11: Audit Controls §164.312(b)

Implement hardware, software, and/or procedures to record and examine information system activity containing or using ePHI.

HIPAA Standard	Tungsten Automation platform
11.1 Hardware (R) —§164.312(b)	Process and procedure, requires measures external to the Tungsten Automation platform.
11.2 Software (R) —§164.312(b)	Process and procedure, requires measures external to the Tungsten Automation platform. Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system.
11.3 Procedures (R) —§164.312(b)	Process and procedure, requires measures external to the Tungsten Automation platform.

Standard 12: Authenticate §164.312(c)(1) and (d)

HIPAA Standard	Tungsten Automation platform
12.1 *Integrity (A)* —§164.312(c)(1) Implement policies and procedures to protect ePHI from improper alteration or destruction.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.2 *Mechanism to Authenticate electronic Protected Health Information (A)* —§164.312(c)(1) Implement electronic mechanisms to validate there is no unauthorized ePHI alteration or destruction.	Process and procedure, requires measures external to the Tungsten Automation platform.
12.3 *Person or Entity Authentication (R)* —§164.312(d) Implement procedures to verify the identity of the person or entity requesting ePHI access.	Process and procedure, requires measures external to the Tungsten Automation platform.

Standard 13: Transmission §164.312(e)(1)

HIPAA Standard	Tungsten Automation platform
13.1 *Integrity Controls (A)* —§164.312(e)(1)(2)(i) Implement security measures to detect improper modification of electronically transmitted ePHI.	Process and procedure, requires measures external to the Tungsten Automation platform.
13.2 *Encryption (A)* —§164.312(e)(1)(2)(ii) Implement a mechanism to encrypt electronic ePHI when needed.	Tungsten Automation platform is certified to operate with IPsec and HTTPS. Supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on mix of Tungsten Automation Products used. Tungsten Automation databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. The full level of SQL encryption is supported. **Note:** If all access is within a secure intranet configuration, encryption may not be required.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) implemented by the European Union (EU)[4] provides data protection law for all EU Member States and gives control of personal data[5] to the owners. The regulation imposes strict rules for institutions and entities who process and host personal data worldwide. Institutions, businesses, and individuals outside of the EU must also abide by the regulations when they collect or process data for any EU citizen.

Under GDPR, EU citizens can:

- Review their stored personal data
- Request and receive corrections to their personal data in a timely manner
- Restrict processing of personal data until its accuracy is verified
- Securely move personal data from one IT source to another
- Invoke their right to be forgotten.

Consent

Before processing personal data, institutions and entities must receive consent. The request for consent must clearly explain how the data will be used and how long it will be stored.

- An individual's inactivity or silence is not sufficient compliance for consent.
- Institutions and entities must prove approval to use an individual's personal information.
- Terms of consent must be accurate with the most up-to-date information and individuals must be informed of any changes to how the data is used.
- Individuals have the right to withdraw consent at any time.
- Institutions and entities must respond to a request to withdraw consent and carry out the request in a reasonable timeframe.

Rectify and amend

Individuals have the right to request corrections and amendments to their personal data. The institution or entity is required to respond to such requests in a timely manner.

Right to be forgotten

Individuals can withdraw consent and request their personal data be deleted. Institutions and entities must remove all traces of the personal data. In addition, data that is no longer used by an institution or entity should be deleted.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[5] Personal data includes, but is not limited to, names, addresses, identification numbers, images, beliefs, geographic location, IP addresses, ethnicity, race, genetic or biometric data, health, and other data that can identify an individual.

Tungsten Automation Products and GDPR Compliance

Compliance

GDPR regulations are broad and wide-ranging. While a number of the requirements involve technology solutions that are addressed directly by the Tungsten Automation platform and the underlying operating system, some require measures external to the Tungsten Automation platform to ensure compliance.

The overall IT ramifications of GDPR are beyond the scope of this document. However, we believe the following topics are key to our customers to meet GDPR requirements for Tungsten Automation Products.

- Data in transit
- Data at rest
- The right to be forgotten
- Permissions

These concepts are covered in the Overview and Tungsten Automation Security Model sections of this document.

Requirements

The following table shows the GDPR Control Objective and associated requirements. The requirements are divided further into more detailed regulations in a subsequent section of this document.

Control Objective	Articles
General Provisions	1. Subject-matter and objectives
	2. Material scope
	3. Territorial scope
	4. Definitions
Principles	5. Processing of personal data
	6. Lawfulness of processing
	7. Conditions for consent
	8. Conditions for child's consent
	9. Processing special categories, personal data
	10. Processing personal data relating to criminal convictions and offenses
	11. Processing which does not require identification
Rights of the data subject	12. Transparency and modalities
	13. Information and access to personal data
	14. Information provided when personal data is not obtained from the data subject
	15. Right of access by the data subject
	16. Right to rectification
	17. Right to erasure (right to be forgotten)
	18. Right to restriction of processing
	19. Notification obligation regarding rectification or erasure of personal data or restriction of processing
	20. Right to data portability
	21. Right to object

Control Objective	Standard
	22. Automated individual decision-making, including profiling
	23. Restrictions
Controller and processor	24. Responsibilities of controllers or processors not established in the Union
	25. Data protection by design and by default
	26. Joint controllers
	27. Representatives of controllers or processors not established in the Union
	28. Processor
	29. Processing under the authority of the controller or processor
	30. Records of processing activities
	31. Cooperation with the supervisory authority
	32. Security of processing
	33. Notification of a personal data breach to the supervisory authority
	34. Communication of a personal data breach to the data subject
	35. Data protection impact assessment
	36. Prior consultation
	37. Designation of the data protection officer
	38. Position of the data protection officer
	39. Tasks of the data protection officer
	40. Codes of conduct
	41. Monitoring of approved codes of conduct
	42. Certification
	43. Certification bodies
Transfers of personal data to third countries or international organizations	44. General principle for transfers
	45. Transfers on the basis of an adequacy decision
	46. Transfers subject to appropriate safeguards
	47. Binding corporate rules
	48. Transfers or disclosures not authorized by Union law
	49. Derogations for specific situations
	50. International cooperation for the protection of personal data
Independent supervisory authorities collapse child menu	51. Supervisory authority
	52. Independence
	53. General conditions for the members of the supervisory authority
	54. Rules on the establishment of the supervisory authority
	55. Competence
	56. Competence of the lead supervisory authority
	57. Tasks
	58. Powers
	59. Activity reports

Control Objective	Standard
Cooperation and consistency	60. Cooperation between the lead supervisory authority and the other supervisory authorities concerned
	61. Mutual assistance
	62. Joint operations of supervisory authorities
	63. Consistency mechanism
	64. Opinion of the Board
	65. Dispute resolution by the Board
	66. Urgency procedure
	67. Exchange of information
	68. European Data Protection Board
	69. Independence
	70. Tasks of the Board
	71. Reports
	72. Procedure
	73. Chair
	74. Tasks of the Chair
	75. Secretariat
	76. Confidentiality
Remedies, liability and penalties collapse child menu	77. Right to lodge a complaint with a supervisory authority
	78. Right to an effective judicial remedy against a supervisory authority
	79. Right to an effective judicial remedy against a controller or processor
	80. Representation of data subjects
	81. Suspension of proceedings
	82. Right to compensation and liability
	83. General conditions for imposing administrative fines
	84. Penalties
Provisions relating to specific - processing situations	85. Processing and freedom of expression and information
	86. Processing and public access to official documents
	87. Processing of the national identification number
	88. Processing in the context of employment
	89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
	90. Obligations of secrecy
	91. Existing data protection rules of churches and religious associations
Delegated acts and implementing acts	92. Exercise of the delegation
	93. Committee procedure
Final Provisions	94. Repeal of Directive 95/46/EC
	95. Relationship with Directive 2002/58/EC
	96. Relationship with previously concluded agreements
	97. Commission reports
	98. Review of other Union legal acts on data protection
	99. Entry into force and application

Regulation 1: General provisions

Rules for the protection of personal data during processing and during the free movement of personal data.

Article 1: Subject-matter and objectives

Applicable GDPR Recitals	Tungsten Automation platform
1. Data protection as a fundamental right Protection of personal data is a fundamental right of individuals.	Process and procedure, requires measures external to the Tungsten Automation platform. Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system as well as numerous other Tungsten Automation Product features. See Overview for additional information.
2. Respect of the fundamental rights and freedoms	Process and procedure, requires measures external to the Tungsten Automation platform.
3. Directive 95/46/EC harmonization Ensure of the free flow of personal data between EU member states when processing personal data.	Process and procedure, requires measures external to the Tungsten Automation platform.
4. Data protection in balance with other fundamental rights Protection of data as balanced against other fundamental rights in accordance with the principal of proportionality.	Process and procedure, requires measures external to the Tungsten Automation platform.
5. Cooperation between Member States to exchange personal data	Process and procedure, requires measures external to the Tungsten Automation platform.
6. Ensuring a high level of data protection despite the increased exchange of data	Process and procedure, requires measures external to the Tungsten Automation platform.
7. The framework is based on control and certainty	Process and procedure, requires measures external to the Tungsten Automation platform.
8. Adoption into national law	Process and procedure, requires measures external to the Tungsten Automation platform.
9. Different standards of protection by the Directive 95/46/EC Consideration of differences in data protection regulations across Member States where differences may constitute and obstacle to the pursuit of economic activities, distort competition, and impede authorities under Union law.	Process and procedure, requires measures external to the Tungsten Automation platform.
10. Harmonized level of data protection despite national scope	Process and procedure, requires measures external to the Tungsten Automation platform.
11. Harmonization of the powers and sanctions	Process and procedure, requires measures external to the Tungsten Automation platform.
12. Authorization of the European Parliament and the Council	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 2: Material scope

Processing of personal data by automated or non-automated means

Applicable GDPR Recitals	Tungsten Automation platform
13. Taking account of micro, small and medium-sized enterprises	Process and procedure, requires measures external to the Tungsten Automation platform.
14. Not applicable to legal persons	Process and procedure, requires measures external to the Tungsten Automation platform.
15. Technology neutrality Protection of personal rights should be technology neutral and not depend on the techniques used.	Process and procedure, requires measures external to the Tungsten Automation platform.
16. Not applicable to activities regarding national and common security	Process and procedure, requires measures external to the Tungsten Automation platform.
17. Adaptation of Regulation (EC) No 45/2001 Applies to the protection of individuals' personal data by Community institutions and Union entities on the free movement of the data.	Process and procedure, requires measures external to the Tungsten Automation platform.
18. Not applicable to personal or household activities The regulation does not apply to the processing of data that is purely personal with no connection to a professional or commercial activity.	Process and procedure, requires measures external to the Tungsten Automation platform.
19. Not applicable to criminal prosecution The regulation does not apply to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.	Process and procedure, requires measures external to the Tungsten Automation platform.
20. Respecting the independence of the judiciary	Process and procedure, requires measures external to the Tungsten Automation platform.
21. Liability rules of intermediary service providers shall remain unaffected	Process and procedure, requires measures external to the Tungsten Automation platform.
27. Not applicable to data of deceased persons	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 3: Territorial scope

The processing of personal data within the EU or external to the EU.

Applicable GDPR Recitals	Tungsten Automation platform
22. Processing by an establishment Processing of personal data in the context of the controller or processor within the Union should be carried out in accordance with this regulation.	Process and procedure, requires measures external to the Tungsten Automation platform.
23. Applicable to processors not established in the Union if data subjects within the Union are targeted Processing of personal data in the context of the controller or processor not established in the union should be carried out in accordance with this regulation.	Process and procedure, requires measures external to the Tungsten Automation platform.
24. Applicable to processors not established in the Union if data subjects within the Union are profiled	Process and procedure, requires measures external to the Tungsten Automation platform.

Applicable GDPR Recitals	Tungsten Automation platform
25. Applicable to processors due to international law	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 4: Definitions

Applicable GDPR Recitals	Tungsten Automation platform
15. Technology neutrality Protection of personal rights should be technology neutral and not depend on the techniques used.	Process and procedure, requires measures external to the Tungsten Automation platform.
24. Applicable to processors not established in the Union if data subjects within the Union are profiled	Process and procedure, requires measures external to the Tungsten Automation platform.
26. Not applicable to anonymous data Identifiable information has been replaced with artificial identifiers or pseudonyms.	Process and procedure, requires measures external to the Tungsten Automation platform.
28. Introduction of pseudonymisation	Process and procedure, requires measures external to the Tungsten Automation platform.
29. Pseudonymisation at the same controller	Process and procedure, requires measures external to the Tungsten Automation platform.
30. Online identifiers for profiling and identifications	Process and procedure, requires measures external to the Tungsten Automation platform.
31. Not applicable to public authorities in connection with their official task	Process and procedure, requires measures external to the Tungsten Automation platform.
34. Genetic data	Process and procedure, requires measures external to the Tungsten Automation platform.
35. Health data	Process and procedure, requires measures external to the Tungsten Automation platform.
36. Determination of the main establishment	Process and procedure, requires measures external to the Tungsten Automation platform.
37. Enterprise group	Process and procedure, requires measures external to the Tungsten Automation platform.

Regulation 2: Principles

Article 5: Principles relating to processing of personal data

Personal data shall be processed lawfully, fairly, with transparency to the individual, limited to the purpose is processed or stored, and ensures appropriate security. Reasonable effort is required to ensure data accuracy and corrections when inaccuracies are known.

Applicable GDPR Recitals	Tungsten Automation platform
39. Principles of data processing	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation products can support these measures as follows: Secure access is supported by authentication and authorization mechanisms within the Tungsten

Applicable GDPR Recitals	Tungsten Automation platform
	Automation platform and Windows operating system. Secure transmission is supported by IPsec, and HTTPS. Secure storage is supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on the mix of Tungsten Automation Products used.

Article 6: Lawfulness of processing

Applicable GDPR Recitals	Tungsten Automation platform
39. Principles of data processing	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation products can support these measures as follows: Secure access is supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system. Secure transmission is supported by IPsec, and HTTPS. Secure storage is supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on the mix of Tungsten Automation Products used.
40. Lawfulness of data processing	Process and procedure, requires measures external to the Tungsten Automation platform.
41. Legal basis or legislative measures	Process and procedure, requires measures external to the Tungsten Automation platform.
42. Burden of proof and requirements for consent	Process and procedure, requires measures external to the Tungsten Automation platform.
43. Freely given consent	Process and procedure, requires measures external to the Tungsten Automation platform.
44. Performance of a contract	Process and procedure, requires measures external to the Tungsten Automation platform.
45. Fulfillment of legal obligations	Process and procedure, requires measures external to the Tungsten Automation platform.
46. Vital interests of the data subject	Process and procedure, requires measures external to the Tungsten Automation platform.
47. Overriding legitimate interest	Process and procedure, requires measures external to the Tungsten Automation platform.
48. Overriding legitimate interest within group of undertakings	Process and procedure, requires measures external to the Tungsten Automation platform.
49. Network and information security as overriding legitimate interest	Process and procedure, requires measures external to the Tungsten Automation platform.
50. Further processing of personal data	Process and procedure, requires measures external to the Tungsten Automation platform.
171. Repeal of Directive 95/46/EC and transitional provisions	Process and procedure, requires measures external

Applicable GDPR Recitals	Tungsten Automation platform
	to the Tungsten Automation platform.

Article 7 – Conditions for consent

Individual consent for the collection and processing of personal data.

Applicable GDPR Recitals	Tungsten Automation platform
32. Consent Collected in a non-ambiguous manner.	Process and procedure, requires measures external to the Tungsten Automation platform.
33. Consent to certain areas of scientific research	Process and procedure, requires measures external to the Tungsten Automation platform.
42. Burden of proof and requirements for consent Held by the institution or entity.	Process and procedure, requires measures external to the Tungsten Automation platform.
43. Freely given consent	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 8 – Conditions applicable to child's consent in relation to information society services

Applicable GDPR Recitals	Tungsten Automation platform
38. Special protection of children's personal data	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 9 – Processing of special categories of personal data

Applicable GDPR Recitals	Tungsten Automation platform
46. Vital interests of the data subject	Process and procedure, requires measures external to the Tungsten Automation platform.
51. Protecting sensitive personal data	Process and procedure, requires measures external to the Tungsten Automation platform.
52. Exceptions to the prohibition on processing special categories of personal data	Process and procedure, requires measures external to the Tungsten Automation platform.
53. Processing of sensitive data in health and social sector	Process and procedure, requires measures external to the Tungsten Automation platform.
54. Processing of sensitive data in public health sector	Process and procedure, requires measures external to the Tungsten Automation platform.
55. Public interest in processing by official authorities for objectives of recognized religious communities	Process and procedure, requires measures external to the Tungsten Automation platform.
56. Processing personal data on people's political opinions by parties	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 10 – Processing of personal data relating to criminal convictions and offences

Applicable GDPR Recitals	Tungsten Automation platform
50. Further processing of personal data	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 11 – Processing which does not require identification

Processing personal data that no longer requires identification of the individual, the institution or entity is not required to maintain, acquire, or process additional information.

Applicable GDPR Recitals	Tungsten Automation platform
57. Additional data for identification purposes	Process and procedure, requires measures external to the Tungsten Automation platform.

Regulation 3: Rights of the data subject

Section 1 – Transparency and modalities

Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

The institution or entity must take appropriate measures to inform the individual in an accessible manner using concise, transparent language.

Applicable GDPR Recitals	Tungsten Automation platform
58. The principle of transparency	Process and procedure, requires measures external to the Tungsten Automation platform.
59. Procedures for the exercise of the rights of the data subjects	Process and procedure, requires measures external to the Tungsten Automation platform.
60. Information obligation	Process and procedure, requires measures external to the Tungsten Automation platform.
73. Restrictions of rights and principles	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 2 – Information and access to personal data

Article 13 – Information to be provided where personal data are collected from the data subject

Applicable GDPR Recitals	Tungsten Automation platform
60. Information obligation	Process and procedure, requires measures external to the Tungsten Automation platform.
61. Time of information	Process and procedure, requires measures external to the Tungsten Automation platform.
62. Exceptions to the obligation to provide information	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 14 – Information to be provided where personal data have not been obtained from the data subject

Applicable GDPR Recitals	Tungsten Automation platform
60. Information obligation	Process and procedure, requires measures external to the Tungsten Automation platform.
61. Time of information	Process and procedure, requires measures external to the Tungsten Automation platform.

Applicable GDPR Recitals	Tungsten Automation platform
62. Exceptions to the obligation to provide information	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 15 – Right of access by the data subject

Applicable GDPR Recitals	Tungsten Automation platform
63. Right of access	Process and procedure, requires measures external to the Tungsten Automation platform.
64. Identity verification	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 3 – Rectification and erasure

Article 16 – Right to rectification

Applicable GDPR Recitals	Tungsten Automation platform
65. Right of rectification and erasure	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this as they support major transaction level system operations (create, read, update, and delete (CRUD)) to ensure field and other data can be modified or deleted as required.

Article 17 – Right to erasure (“right to be forgotten”)

Applicable GDPR Recitals	Tungsten Automation platform
65. Right of rectification and erasure	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this as they support major transaction level system operations (create, read, update, and delete (CRUD)) to ensure field and other data can be modified or deleted as required.
66. Right to be forgotten	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this as they support major transaction level system operations (create, read, update, and delete (CRUD)) to ensure field and other data can be modified or deleted as required.

Article 18 – Right to restriction of processing

Applicable GDPR Recitals	Tungsten Automation platform
67. Restriction of processing	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of

processing

Applicable GDPR Recitals	Tungsten Automation platform
66. Right to be forgotten	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this. See Right to rectification for additional information.

Article 20 – Right to data portability

Applicable GDPR Recitals	Tungsten Automation platform
68. Right of data portability	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this via support for numerous export formats including in both human and machine readable formats such as text, Microsoft Excel, email, and others. See specific product documentation for more information on available features applicable to export.

Section 4 – Right to object and automated individual decision-making

Article 21 – Right to object

Applicable GDPR Recitals	Tungsten Automation platform
69. Right to object	Process and procedure, requires measures external to the Tungsten Automation platform.
70. Right to object to direct marketing	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 22 – Automated individual decision-making, including profiling

Applicable GDPR Recitals	Tungsten Automation platform
71. Profiling	Process and procedure, requires measures external to the Tungsten Automation platform.
72. Guidance of the European Data Protection Board regarding profiling	Process and procedure, requires measures external to the Tungsten Automation platform.
91. Necessity of a data protection impact assessment	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 5 – Restrictions

Article 23 – Restrictions

An institution or entity may restrict the scope of the obligations and rights through legislative measures in cases of national security, defense, and public security, investigation of criminal offences, matters of public health, or judicial proceedings.

Applicable GDPR Recitals	Tungsten Automation platform
73. Restriction of rights and principles	Process and procedure, requires measures external to the Tungsten Automation platform.

Regulation 4: Controller and processor

Section 1 – General obligations

Article 24 – Responsibility of the controller

Applicable GDPR Recitals	Tungsten Automation platform
74. Responsibility and liability of the controller	Process and procedure, requires measures external to the Tungsten Automation platform.
75. Risks to the rights and freedoms of natural persons	Process and procedure, requires measures external to the Tungsten Automation platform.
76. Risk assessment	Process and procedure, requires measures external to the Tungsten Automation platform.
77. Risk assessment guidelines	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 25 – Data protection by design and by default

Applicable GDPR Recitals	Tungsten Automation platform
78. Appropriate technical and organizational measures	Supported by Tungsten Automation platform in conjunction with Windows operating system and measures external to the Tungsten Automation platform.

Article 26 – Joint controllers

Applicable GDPR Recitals	Tungsten Automation platform
79. Allocation of the responsibilities	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 27 – Representatives of controllers or processors not established in the Union

Applicable GDPR Recitals	Tungsten Automation platform
80. Designation of a representative	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 28 – Processor

Institution or entity's use of processors must implement appropriate technical and organizational measures are followed to ensure the protection of the rights of the individual.

Applicable GDPR Recitals	Tungsten Automation platform
81. The use of processors	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 29 – Processing under the authority of the controller or processor

Process and procedure, requires measures external to the Tungsten Automation platform.

Article 30 – Records of processing activities

Institutions and entities shall maintain record of processing activities under its responsibility.

Applicable GDPR Recitals	Tungsten Automation platform
13. Taking account of micro, small and medium-sized enterprises	Process and procedure, requires measures external to the Tungsten Automation platform.
82. Record of processing activities	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this. See Accountability for additional information.

Article 31 – Cooperation with the supervisory authority

Institutions and entities shall cooperate on request with supervisory authority in the performance of its tasks.

Applicable GDPR Recitals	Tungsten Automation platform
82. Record of processing activities	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this. See Accountability for additional information.

Section 2 – Security of personal data

Article 32 – Security of processing

Institutions and entities shall implement appropriate measures to ensure an appropriate level of security.

Applicable GDPR Recitals	Tungsten Automation platform
75. Risks to the rights and freedoms of natural persons	Process and procedure, requires measures external to the Tungsten Automation platform.
76. Risk assessment	Process and procedure, requires measures external to the Tungsten Automation platform.
77. Risk assessment guidelines	Process and procedure, requires measures external to the Tungsten Automation platform.
78. Appropriate technical and organizational measures	Process and procedure, requires measures external to the Tungsten Automation platform.
79. Allocation of the responsibilities	Process and procedure, requires measures external to the Tungsten Automation platform.
83. Security of processing	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation products can support these measures as follows: Secure access is supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system. Secure transmission is supported by IPsec, and HTTPS. Secure storage is supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on the mix of Tungsten Automation Products used.

Article 33 – Notification of a personal data breach to the supervisory authority

Institutions and entities shall notify individuals of any personal data breach without undue delay.

Applicable GDPR Recitals	Tungsten Automation platform
85. Notification obligation of breaches to the supervisory authority	Process and procedure, requires measures external to the Tungsten Automation platform.
87. Promptness of reporting / notification	Process and procedure, requires measures external to the Tungsten Automation platform.
88. Format and procedures of the notification	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 34 – Communication of a personal data breach to the data subject

Applicable GDPR Recitals	Tungsten Automation platform
86. Notification obligation of breaches to the supervisory authority	Process and procedure, requires measures external to the Tungsten Automation platform.
87. Notification of data subjects in case of data breaches	Process and procedure, requires measures external to the Tungsten Automation platform.
88. Promptness of reporting / notification	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 3 – Data protection impact assessment and prior consultation

Article 35 – Data protection impact assessment

Applicable GDPR Recitals	Tungsten Automation platform
75. Risks to the rights and freedoms of natural persons	Process and procedure, requires measures external to the Tungsten Automation platform.
84. Risk evaluation and impact assessment	Process and procedure, requires measures external to the Tungsten Automation platform.
89. Elimination of the general reporting requirement	Process and procedure, requires measures external to the Tungsten Automation platform.
90. Data protection impact assessment	Process and procedure, requires measures external to the Tungsten Automation platform.
91. Necessity of a data protection impact assessment	Process and procedure, requires measures external to the Tungsten Automation platform.
92. Broader data protection impact assessment	Process and procedure, requires measures external to the Tungsten Automation platform.
93. Data protection impact assessment at authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 36 – Prior consultation

Applicable GDPR Recitals	Tungsten Automation platform
94. Consultation of the supervisory authority	Process and procedure, requires measures external to the Tungsten Automation platform.
95. Support by the processor	Process and procedure, requires measures external

Applicable GDPR Recitals	Tungsten Automation platform
	to the Tungsten Automation platform.
96. Consultation of the supervisory authority in the course of a legislative process	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 4 – Data protection officer

Article 37 – Designation of the data protection officer

Applicable GDPR Recitals	Tungsten Automation platform
97. Data protection officer	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 38 – Position of the data protection officer

Applicable GDPR Recitals	Tungsten Automation platform
97. Data protection officer	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 39 – Tasks of the data protection officer

Applicable GDPR Recitals	Tungsten Automation platform
97. Data protection officer	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 5 – Codes of conduct and certification

Article 40 – Codes of conduct

Applicable GDPR Recitals	Tungsten Automation platform
98. Preparation of codes of conduct by organizations and associations	Process and procedure, requires measures external to the Tungsten Automation platform.
99. Consultation of stakeholders and data subjects in the development of codes of conduct	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 41 – Monitoring of approved codes of conduct

No applicable regulations associated with this Article.

Article 42 – Certification

Member States and supervisory authorities shall encourage establishment of data protection certification for the purpose of demonstrating compliance.

Applicable GDPR Recitals	Tungsten Automation platform
100. Certification	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 43 – Certification bodies

Note: Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

Regulation 5: Transfers of personal data to third countries or international organizations

Article 44 – General principle for transfers

Institutions and entities should get an individual's permission before transferring data.

Applicable GDPR Recitals	Tungsten Automation platform
101. General principles for international data transfers	Process and procedure, requires measures external to the Tungsten Automation platform.
102. International agreements for an appropriate level of data protection	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 45 – Transfers on the basis of an adequacy decision

Applicable GDPR Recitals	Tungsten Automation platform
103. Appropriate level of data protection based on an adequacy decision	Process and procedure, requires measures external to the Tungsten Automation platform.
104. Criteria for an adequacy decision	Process and procedure, requires measures external to the Tungsten Automation platform.
105. Consideration of international agreements for an adequacy decision	Process and procedure, requires measures external to the Tungsten Automation platform.
106. Monitoring and periodic review of the level of data protection	Process and procedure, requires measures external to the Tungsten Automation platform.
107. Amendment, revocation and suspension of adequacy decisions	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 46 – Transfers subject to appropriate safeguards

Applicable GDPR Recitals	Tungsten Automation platform
108. Appropriate safeguards	Process and procedure, requires measures external to the Tungsten Automation platform.
109. Standard data protection clauses	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 47 – Binding corporate rules

Applicable GDPR Recitals	Tungsten Automation platform
110. Binding corporate rules	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 48 – Transfers or disclosures not authorized by Union law

Applicable GDPR Recitals	Tungsten Automation platform
115. Rules in third countries contrary to the Regulation	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 49 – Derogations for specific situations

Applicable GDPR Recitals	Tungsten Automation platform
111. Exceptions for certain cases of international transfers	Process and procedure, requires measures external to the Tungsten Automation platform.
112. Data transfers due to important reasons of public interest	Process and procedure, requires measures external to the Tungsten Automation platform.
113. Transfers qualified as not repetitive and that only concern a limited number of data subjects	Process and procedure, requires measures external to the Tungsten Automation platform.
114. Safeguarding of enforceability of rights and obligations in the absence of an adequacy decision	Process and procedure, requires measures external to the Tungsten Automation platform.
115. Rules in third countries contrary to the Regulation	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 50 – International cooperation for the protection of personal data

Applicable GDPR Recitals	Tungsten Automation platform
116. Cooperation among supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Regulation 6: Independent supervisory authorities

Section 1 – Independent status

The agency that monitors GDPR within a country.

Article 51 – Supervisory authority

Applicable GDPR Recitals	Tungsten Automation platform
117. Establishment of supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
118. Monitoring of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
119. Organization of several supervisory authorities of a Member State	Process and procedure, requires measures external to the Tungsten Automation platform.
120. Features of supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 52 – Independence

Applicable GDPR Recitals	Tungsten Automation platform
117. Establishment of supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
118. Monitoring of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
120. Features of supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Applicable GDPR Recitals	Tungsten Automation platform
121. Independence of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 53 – General conditions for the members of the supervisory authority

Applicable GDPR Recitals	Tungsten Automation platform
121. Independence of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 54 – Rules on the establishment of the supervisory authority

Applicable GDPR Recitals	Tungsten Automation platform
117. Establishment of supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
121. Independence of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 2 – Competence, tasks and powers

Regulatory authorities within a country should have sufficient expertise in technical areas such as encryption, data storage, and data transfer.

Article 55 – Competence

Applicable GDPR Recitals	Tungsten Automation platform
122. Independence of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 56 – Competence of the lead supervisory authority

Applicable GDPR Recitals	Tungsten Automation platform
124. Lead authority regarding processing in several Member States	Process and procedure, requires measures external to the Tungsten Automation platform.
127. Information of the supervisory authority regarding local processing	Process and procedure, requires measures external to the Tungsten Automation platform.
128. Responsibility regarding processing in the public interest	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 57 – Tasks

Applicable GDPR Recitals	Tungsten Automation platform
122. Responsibility of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
123. Cooperation of the supervisory authorities with each other and with the Commission	Process and procedure, requires measures external to the Tungsten Automation platform.
132. Awareness-raising activities and specific measures	Process and procedure, requires measures external to the Tungsten Automation platform.
133. Mutual assistance and provisional measures	Process and procedure, requires measures external

Applicable GDPR Recitals	Tungsten Automation platform
	to the Tungsten Automation platform.
137. Provisional measures	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 58 – Powers

Applicable GDPR Recitals	Tungsten Automation platform
122. Responsibility of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
129. Tasks and powers of the supervisory authorities	Process and procedure, requires measures external to the Tungsten Automation platform.
131. Attempt of an amicable settlement	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 59 – Activity reports

No applicable regulations associated with this Article.

Regulation 7: Cooperation and consistency

Section 1 – Cooperation

Article 60 – Cooperation between the lead supervisory authority and the other supervisory authorities concerned

Applicable GDPR Recitals	Tungsten Automation platform
124. Lead authority regarding processing in several Member States	Process and procedure, requires measures external to the Tungsten Automation platform.
125. Competences of the lead authority	Process and procedure, requires measures external to the Tungsten Automation platform.
130. Consideration of the authority with which the complaint has been lodged	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 61 – Mutual assistance

Applicable GDPR Recitals	Tungsten Automation platform
123. Cooperation of the supervisory authorities with each other and with the Commission	Process and procedure, requires measures external to the Tungsten Automation platform.
132. Awareness-raising activities and specific measures	Process and procedure, requires measures external to the Tungsten Automation platform.
133. Mutual assistance and provisional measures	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 62 – Joint operations of supervisory authorities

Applicable GDPR Recitals	Tungsten Automation platform
126. Joint decisions	Process and procedure, requires measures external

Applicable GDPR Recitals	Tungsten Automation platform
	to the Tungsten Automation platform.
134. Participation in joint operations	Process and procedure, requires measures external to the Tungsten Automation platform.

Section 2 – Consistency

Article 63 – Consistency mechanism

Applicable GDPR Recitals	Tungsten Automation platform
135. Consistency mechanism	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 64 – Opinion of the Board

Applicable GDPR Recitals	Tungsten Automation platform
136. Binding decisions and opinions of the Board	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 65 – Dispute resolution by the Board

Applicable GDPR Recitals	Tungsten Automation platform
136. Binding decisions and opinions of the Board	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 66 – Urgency procedure

Applicable GDPR Recitals	Tungsten Automation platform
137. Provisional measures	Process and procedure, requires measures external to the Tungsten Automation platform.
138. Urgency procedure	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 67 – Exchange of information

Refers to the standardized format defined in Article 63 and implemented in Article 93(2).

Section 3 – European data protection board

Article 68 – European Data Protection Board

Applicable GDPR Recitals	Tungsten Automation platform
139. European Data Protection Board	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 69 – Independence

Applicable GDPR Recitals	Tungsten Automation platform
139. European Data Protection Board	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 70 – Tasks of the Board

Applicable GDPR Recitals	Tungsten Automation platform
136. Binding decisions and opinions of the Board	Process and procedure, requires measures external to the Tungsten Automation platform.
139. European Data Protection Board	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 71 – Reports

Defines activities of the European Data Protection Board that are external to the Tungsten Automation platform.

Article 72 – Procedure

Defines activities of the European Data Protection Board that are external to the Tungsten Automation platform.

Article 73 – Chair

Defines activities of the European Data Protection Board that are external to the Tungsten Automation platform.

Article 74 – Tasks of the Chair

Defines activities of the European Data Protection Board that are external to the Tungsten Automation platform.

Article 75 – Secretariat

Applicable GDPR Recitals	Tungsten Automation platform
140. Secretariat and staff of the Board	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 76 – Confidentiality

Defines activities of the European Data Protection Board that are external to the Tungsten Automation platform.

Regulation 8: Remedies, liability and penalties

Article 77 – Right to lodge a complaint with a supervisory authority

Applicable GDPR Recitals	Tungsten Automation platform
141. Right to lodge a complaint	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 78 – Right to an effective judicial remedy against a supervisory authority

Applicable GDPR Recitals	Tungsten Automation platform
141. Right to lodge a complaint	Process and procedure, requires measures external to the Tungsten Automation platform.
143. Judicial remedies	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 79 – Right to an effective judicial remedy against a controller or processor

Applicable GDPR Recitals	Tungsten Automation platform
141. Right to lodge a complaint	Process and procedure, requires measures external to the Tungsten Automation platform.
145. Choice of venue	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 80 – Representation of data subjects

Applicable GDPR Recitals	Tungsten Automation platform
142. The right of data subjects to mandate a not-for-profit body, organization or association	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 81 – Suspension of proceedings

Applicable GDPR Recitals	Tungsten Automation platform
144. Related proceedings	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 82 – Right to compensation and liability

Applicable GDPR Recitals	Tungsten Automation platform
145. Choice of venue	Process and procedure, requires measures external to the Tungsten Automation platform.
146. Indemnity	Process and procedure, requires measures external to the Tungsten Automation platform.
147. Jurisdiction	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 83 – General conditions for imposing administrative fines

Applicable GDPR Recitals	Tungsten Automation platform
148. Penalties	Process and procedure, requires measures external to the Tungsten Automation platform.
149. Penalties for infringements of national rules	Process and procedure, requires measures external to the Tungsten Automation platform.
150. Administrative fines	Process and procedure, requires measures external to the Tungsten Automation platform.
151. Administrative fines in Denmark and Estonia	Process and procedure, requires measures external to the Tungsten Automation platform.
152. Power of sanction of the Member States	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 84 – Penalties

Applicable GDPR Recitals	Tungsten Automation platform
149. Penalties for infringements of national rules	Process and procedure, requires measures external to the Tungsten Automation platform.

Applicable GDPR Recitals	Tungsten Automation platform
150. Administrative fines	Process and procedure, requires measures external to the Tungsten Automation platform.
151. Administrative fines in Denmark and Estonia	Process and procedure, requires measures external to the Tungsten Automation platform.
152. Power of sanction of the Member States	Process and procedure, requires measures external to the Tungsten Automation platform.

Regulation 9: Provisions relating to specific processing situations

Article 85 – Processing and freedom of expression and information

Applicable GDPR Recitals	Tungsten Automation platform
153. Processing of personal data solely for journalistic purposes or for the purposes of academic, artistic or literary expression	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 86 – Processing and public access to official documents

Applicable GDPR Recitals	Tungsten Automation platform
154. Principle of public access to official documents	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 87 – Processing of the national identification number

Defines activities of Member States that are external to the Tungsten Automation platform.

Article 88 – Processing in the context of employment

Applicable GDPR Recitals	Tungsten Automation platform
155. Processing in the employment context	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 89 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Applicable GDPR Recitals	Tungsten Automation platform
156. Processing for archiving, scientific or historical research or statistical purposes	Process and procedure, requires measures external to the Tungsten Automation platform.
157. Information from registries and scientific research	Process and procedure, requires measures external to the Tungsten Automation platform.
158. Processing for archiving purposes	Process and procedure, requires measures external to the Tungsten Automation platform.
159. Processing for scientific research purposes	Process and procedure, requires measures external to the Tungsten Automation platform.
160. Processing for historical research purposes	Process and procedure, requires measures external to the Tungsten Automation platform.
161. Consenting to the participation in clinical trials	Process and procedure, requires measures external to the Tungsten Automation platform.

Applicable GDPR Recitals	Tungsten Automation platform
162. Processing for statistical purposes	Process and procedure, requires measures external to the Tungsten Automation platform.
163. Production of European and national statistics	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 90 – Obligations of secrecy

Applicable GDPR Recitals	Tungsten Automation platform
164. Professional or other equivalent secrecy obligations	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 91 – Existing data protection rules of churches and religious associations

Applicable GDPR Recitals	Tungsten Automation platform
165. No prejudice of the status of churches and religious associations	Process and procedure, requires measures external to the Tungsten Automation platform.

Regulation 10: Delegated acts and implementing acts

Article 92 – Exercise of the delegation

Applicable GDPR Recitals	Tungsten Automation platform
166. Delegated acts of the Commission	Process and procedure, requires measures external to the Tungsten Automation platform.
167. Implementing powers of the Commission	Process and procedure, requires measures external to the Tungsten Automation platform.
168. Implementing acts on standard contractual clauses	Process and procedure, requires measures external to the Tungsten Automation platform.
169. Immediately applicable implementing acts	Process and procedure, requires measures external to the Tungsten Automation platform.
170. Principle of subsidiarity and principle of proportionality	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 93 – Committee procedure

Defines activities of the Commission that are external to the Tungsten Automation platform.

Regulation 11: Final provisions

Article 94 – Repeal of Directive 95/46/EC

GDPR cancels this earlier EU regulation.

Applicable GDPR Recitals	Tungsten Automation platform
171. Repeal of Directive 95/46/EC and transitional provisions	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 95 – Relationship with Directive 2002/58/EC

GDPR integrates with this earlier EU regulation.

Applicable GDPR Recitals	Tungsten Automation platform
173. Relationship to Directive 2002/58/EC	Process and procedure, requires measures external to the Tungsten Automation platform.

Article 96 – Relationship with previously concluded Agreements

GDPR cancels previous international agreements.

Process and procedure, requires measures external to the Tungsten Automation platform.

Article 97 – Commission reports

The Commission is required to report on GDPR every four years.

Process and procedure, requires measures external to the Tungsten Automation platform.

Article 98 – Review of other Union legal acts on data protection

Process and procedure, requires measures external to the Tungsten Automation platform.

Article 99 – Entry into force and application

GDPR effective date – May 25, 2018.

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) is a state law intended to enhance privacy rights and consumer protection for residents of California in the United States. CCPA applies to any person or entity that conducts business in California and satisfies at least one of the following requirements:

- Has annual gross revenues in excess of $25 million
- Buys, receives, or sells the personal information of 50,000 or more consumers or households
- Earns more than half of its annual revenue from selling consumers' personal information

Privacy rights

Under CCPA, consumers have certain rights related to their personal information collected by and on behalf of a business subject to the law. Personal information may include data elements such as geolocation, IP address, biometric information, professional or employment-related information, education information, browsing and search history, and other noted types of data.

Consumers have certain rights under CCPA to expect that businesses implement reasonable security, as outlined in the following sections.

Right to know personal information

Under CCPA, California residents may request a business to disclose the following information about the business' collection and use of their personal information over the past twelve (12) months, provided that such requests are made no more than twice within a twelve (12) month period:

- The categories of personal information collected
- The categories of sources for the personal information collected
- The business or commercial purpose for collecting, and, if applicable, selling, personal information
- The specific pieces of personal information collected
- If the personal information has been disclosed, the categories of personal information disclosed and the categories of third parties receiving the personal information
- If the personal information has been sold, the categories of personal information sold and the categories of third parties to whom the personal information was sold.

Right of deletion

California residents may request a business to delete the personal information that the business collected and has been retained by the business or its service providers. This right is limited, and the business may deny a deletion request if it is necessary for the business or a service provider to maintain the personal information in order to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by the individual, or reasonably anticipated within the context of a business'

ongoing business relationship with the individual, or otherwise perform a contract between the business and the individual.

- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, where the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the individual has provided informed consent.
- Enable solely internal uses that are reasonably aligned with the expectations of the individual based on the individual's relationship with the business.
- Comply with a legal obligation.
- Otherwise use the individual's personal information, internally, in a lawful manner that is compatible with the purpose for which the individual provided the information.

Right of no sale of personal information

A California resident has the right to opt-out of the sale of their Personal Information by a business subject to the CCPA. In addition, a business subject to the CCPA must have affirmative authorization in order to sell the Personal Information of a California resident who it knows is under the age of 16.

Right of Non-Discrimination

A business subject to the CCPA may not discriminate against a California resident for exercising any of their CCPA privacy rights.

Tungsten Automation platform and CCPA Compliance

Compliance

CCPA regulations are broad and wide-ranging. While some CCPA requirements involve technology solutions addressed directly by the Tungsten Automation platform and the underlying operating system, most require measures external to the Tungsten Automation platform to ensure compliance.

The overall IT ramifications of CCPA are beyond the scope of this document. However, we believe the following topics are key to our customers to meet CCPA requirements for Tungsten Automation Products.

- Data in transit
- Data at rest
- Data privacy rights
- Permissions

These concepts are covered in the Overview and Tungsten Automation Security Model sections of this document.

Requirements

Under CCPA, organizations are expected to implement a certain level of controls that enforce reasonable security relative to collection or maintenance of personal information. The following table shows the minimum level of Center for Internet Security (CIS) Controls that must be implemented under CCPA.

CIS Control Title	Action	CIS Control References
General Provisions	Know the hardware and software connected to your network.	CSC 1, CSC 2
Configure Securely	Implement key security settings.	CSC 3, CSC 11
Control Users	Limit user and administrator privileges.	CSC 5, CSC 14
Update Continuously	Continuously assess vulnerabilities and patch holes to stay current.	CSC 4
Protect Key Assets	Secure critical assets and attack vectors.	CSC 7, CSC 10, CSC 13
Implement Defenses	Defend against malware and boundary intrusions.	CSC 8, CSC 12
Block Access	Block vulnerable access points.	CSC 9, CSC 15, CSC 18
Train Staff	Provide security training to employees, contractors and any vendors with access.	CSC 17
Monitor Activity	Monitor accounts and network audit logs.	CSC 6, CSC 16
Test and Plan Response	Conduct tests of your defenses and be prepared to respond promptly and effectively to security incidents.	CSC 19, CSC 20

Recommended measures

In addition to CIS Controls, the California Attorney General has recommended implementation of three measures listed in the following table.

Title	Action
Multi-Factor Authentication	Multi-factor authentication should be available to consumer-facing online accounts in addition to employee systems. Multi-factor authentication pairs “something you know,” such as a password or PIN, with “something you are or have,” such as your cell phone or fingerprint.
Encryption of Data on Portable Devices	Use encryption on laptops and other portable devices.
Fraud Alerts	Inform consumers about placing a fraud alert on their credit files when there is a breach.

CCPA requirements and Tungsten Automation platform

This section summarizes how CCPA requirements are addressed by the Tungsten Automation platform.

CCPA Requirement	Tungsten Automation platform
General Provisions, CSC 1, CSC 2 Know the hardware and software connected to your network.	Process and procedure, requires measures external to the Tungsten Automation platform. See Security Development Lifecycle for more information about implementation and methodology applied during development of Tungsten Automation products. Also see Secure Operational Process.
Configure Securely, CSC 3, CSC 11 Implement key security settings.	Tungsten Automation platform is certified to operate with IPsec and HTTPS. Supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on mix of Tungsten Automation Products used. Tungsten Automation databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. The full level of SQL encryption is supported. Note: If all access is within a secure intranet configuration, encryption may not be required. Also see Secure Operational Process.
Control Users, CSC 5, CSC 14 Limit user and administrator privileges.	Supported by authentication and authorization mechanisms within the Tungsten Automation platform and Windows operating system as well as numerous other Tungsten Automation Product features. See Overview for additional information. Note: Tungsten Automation Products provide user management that allows restricting access to any information stored by Tungsten Automation.
Update Continuously, CSC 4 Continuously assess vulnerabilities and patch holes to stay current.	Tungsten Automation supports several features and add-on products that can be used for auditing and reporting purposes. See Auditing and Reporting and Login Audits for more information.
Protect Key Assets, CSC 7, CSC 10, CSC 13 Secure critical assets and attack vectors.	Process and procedure, requires measures external to the Tungsten Automation platform.
Implement Defenses, CSC 8, CSC 12 Defend against malware and boundary intrusions.	Process and procedure, requires measures external to the Tungsten Automation platform.

CCPA Requirement	Tungsten Automation platform
Block Access, CSC 9, CSC 15, CSC 18 Block vulnerable access points.	Process and procedure, requires measures external to the Tungsten Automation platform. Supported by Tungsten Automation platform in conjunction with Windows operating system. See Login Audits for more information.
Train Staff, CSC 17 Provide security training to employees, contractors and any vendors with access.	Process and procedure, requires measures external to the Tungsten Automation platform.
Monitor Activity, CSC 6, CSC 16 Monitor accounts and network audit logs.	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this. See Accountability for additional information.
Test and Plan Response, CSC 19, CSC 20 Conduct tests of your defenses and be prepared to respond promptly and effectively to security incidents.	Process and procedure, requires measures external to the Tungsten Automation platform. The Tungsten Automation platform can help support this. See Accountability for additional information.
Multi-Factor Authentication Multi-factor authentication should be available to consumer-facing online accounts in addition to employee systems. Multi-factor authentication pairs “something you know,” such as a password or PIN, with “something you are or have,” such as your cell phone or fingerprint.	Supported by authentication and authorization mechanisms from the Windows operating system. See Overview for additional information. Note: Tungsten Automation products provide user management that allows restricting access to any information stored by Tungsten Automation as linked or synchronized to users in the Windows operating system.
Encryption of Data on Portable Devices Use encryption on laptops and other portable devices.	Tungsten Automation platform is certified to operate with IPsec and HTTPS. Supported through correct implementation of folder based encryption using Microsoft EFS and/or database encryption depending on the mix of Tungsten Automation Products used. Tungsten Automation databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. The full level of SQL encryption is supported. Note: If all access is within a secure intranet configuration, encryption may not be required.
Fraud Alerts Inform consumers about placing a fraud alert on their credit files when there is a breach.	Process and procedure, requires measures external to the Tungsten Automation platform.