Wincanton

Supplier Information Security Policy

Version:	1.1
First Published:	7 June 2021
EMT Owner:	Group CIO
Document:	ITAPI.01.03.Supplier IT Security.POLICY

Contents

Version Control

Version	Date	Updated by	Reason for Update	Status
V0.1	27 May 2021	Jamie Salvage	First draft	Draft
V1.0	7 June 2021	Jamie Salvage	Final	Published
V1.1	21 June 2021	Jamie Salvage	Minor adjustments based on CIO feedback	Published

Supplier Information Security Policy

Control	Description	Importance
Information Security Governance Framework	The Supplier must have an established and consistent industry standard security framework for Information Security governance The Supplier must have an established a security program to protect the Supplier from Cyber threats in accordance with Leading Industry Practice (including NIST, Cyber Essentials Plus, ISO/IEC 27001) or applicable industry requirements. The Security governance framework must be developed, documented, approved, and implemented which includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The Supplier should ensure that there is individual accountability for information and systems by ensuring that there is appropriate ownership of critical business environments, information and systems and that this is assigned to capable individuals.	If this principle is not implemented, Wincanton, its Suppliers or Customers may not have and be able to demonstrate appropriate oversight of Information/Cyber security. A strong security governance framework sets the security tone for the whole organisation.
Information Security Risk Management	The Supplier must establish a security risk management program that effectively evaluates, mitigates, and monitors security risks across the supplier-controlled environment. The likelihood and impact associated with inherent and residual risk must be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance). The Supplier must perform as a minimum an annual security risk assessment in relation to Information/Cyber security and based on the specific environments, consider a more frequent cadence. The Supplier must notify Wincanton, within a reasonable timeframe, if they are unable to remediate or significantly reduce any material areas of risk that could impact the service being provided to Wincanton.	Documented policies and standards are crucial elements for risk management and governance. They set the management's view of the controls required to manage information/cyber risk. If this principle is not implemented, then Wincanton information may be inappropriately disclosed and/or there may be loss of service leading to legal and regulatory sanction or reputational damage.

Approved Usage	The Supplier must produce and publish acceptable use policy informing supplier personnel of their responsibilities. The Supplier must take appropriate steps to ensure compliance to the acceptable use policy.	An acceptable use policy helps to underpin the control environment protecting Information Assets.
Awareness, Behaviour and Culture	The Supplier must have a security awareness training program established for all employees, contractors, and third-party users of the organization's systems and mandated when appropriate. All individuals with access to Wincanton data/ information must receive appropriate awareness training and regular updates in organisational procedures, processes, and policies relating to their professional function relative to the organisation. The levels of training and awareness must be commensurate to the roles being undertaken and recorded in a suitable learning management platform. Supplier must ensure that all personnel under their control undertake mandatory security information training, which includes Cyber Security best practice and protection.	Awareness, behavioural and cultural controls support all other controls within this schedule. If this principle is not implemented, relevant employees will be unaware of cyber risks and attack vectors and would be unable to detect or prevent attacks.
Information Security Incident Management	The Supplier must establish an Information Security incident management framework that effectively validates, contains, and removes / mitigates a security incident from the supplier environment. The Supplier must ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management: The Supplier must ensure that response activities are improved through incorporating lessons learned from current and previous detection/response activities. The Supplier should ensure that incident response teams and processes are tested, at least annually, to ensure the Supplier is able to respond to Cyber security incidents. The Supplier must appoint a Point of Contact for any security incidents who will liaise with Wincanton in the event of an incident. The Supplier must notify Wincanton of the individual(s) contact details and any changes to them, including any out of hours' contacts and telephone numbers. The Supplier will inform the Wincanton, within a reasonable timeframe upon becoming aware of any incident that impacts the service to Wincanton or Wincanton information/data. In the event of either a suspected or known data breach the vendor shall inform Wincanton of such incidents in line with the impacted data protection legislation. Information Security incidents should be reported to the Wincanton IT Security IT.Security@Wincanton.co.uk Data Protection incidents should be reported to the Wincanton Data Protection Officer DPO@Wincanton.co.uk	An information security incident management and response process help to ensure that incidents are quickly contained, and exposure is mitigated.

Information Classification and Protection	The Supplier must have an established and implemented an appropriate information classification and handling framework (aligned to Good Industry Practice) which covers the following: • Assigning the correct information label. • Handling Information securely in line with its assigned level of classification. · • Labelling and handling requirements and how to correctly apply the correct information classification. The Supplier must refer to the Wincanton’s Data Classification and Handling Requirements (Appendix A), or an alternative scheme to ensure that Supplier protects and secures the Wincanton Information held and/or processed. This requirement applies to all Information Assets held and/or processed on behalf of Wincanton.	Appropriate controls must be operated effectively in order to ensure that Wincanton’s sensitive information is restricted to those who should be allowed to access it (confidentiality), protected from unauthorised changes (integrity) and can be retrieved and presented when it is required (availability). If these requirements are not implemented, it may result in Wincanton’s sensitive information being vulnerable to unauthorized modification, disclosure, access, damage, loss or destruction, which may result in legal and regulatory sanction, reputational damage, or loss / disruption of business.
Asset Management	The Supplier must ensure an effective asset management program is established throughout the asset lifecycle. Asset management should govern the lifecycle of assets from acquisition to retirement, providing visibility and security to all asset classes in the environment. The Supplier must maintain a complete and accurate inventory of business-critical assets located at all sites and/or geographical locations which provide service(s) to Wincanton and including any Wincanton equipment hosted in supplier premises, a subcontractor of the vendor or provided by Wincanton, and ensure that there is at least one test annually to validate that the Information asset inventory is current, complete and accurate. Asset Management process should cover the following areas: • Information Assets and Infrastructure are protected based on their classification • Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information • Ensure that unauthorised assets are either removed from the network, quarantined or the inventory is updated in a timely manner • Maintain an up-to-date list of all authorized software that is required for Wincanton’s service delivery. • Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organisation’s authorised software inventory. Unsupported software should be tagged as unsupported in the inventory system. The Supplier should ensure effective and efficient procedures are implemented for the mitigation of non-supported technologies and the end-of-life, retirement, and destruction of assets and data to eliminate the risk of data compromise.	A complete and accurate inventory of Information assets is essential for ensuring appropriate controls. If this principle is not implemented, Wincanton’s assets or assets used by Suppliers to service Wincanton could be compromised, which may result in financial losses, loss of data, reputational damage and regulatory breach.

Destruction, Deletion and Decommission of Physical and Logical Information	Wincanton Information Assets stored in either physical or electronic form, when being destroyed or deleted must be performed in a secure way appropriate to its associated risk, ensuring that Wincanton data is not recoverable. The Supplier should establish policies and procedures with supporting business processes and technical measures implemented for the secure disposal and complete removal of Wincanton data from all storage media, ensuring data is not recoverable by any computer forensic means	Secure destruction of Information Assets helps to ensure that Wincanton Information assets cannot be recovered for any data breach or loss or malicious activity.
Boundary and Network Security	The Supplier must ensure that all IT Systems operated by the Supplier or its sub-contractor that support services provided to Wincanton are protected from lateral movement of threats within the Suppliers (and any relevant sub-contractors') network. The supplier must detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data. The Suppliers networks must be protected through applying defence-in-depth principles, including but not limited to network segmentation, physical access controls to network and the use of strong network firewall capabilities. The Supplier must have network intrusion prevention technologies to detect and prevent malicious traffic from entering the network. The Supplier must ensure all configuration rules that allow traffic to flow through network devices are documented in a configuration management system with a specific business reason for each rule. The Supplier must perform regular scans from outside each trusted network boundary to detect any unauthorised connections which are accessible across the boundary. The Supplier must secure communications between devices and management stations/consoles. · The Supplier must review the firewall (External and Internal Firewall) rules on an annual basis. The Supplier must ensure that access to the internal network must be monitored and only authorised devices must be allowed through appropriate network access controls The Supplier must ensure that remote login access to the supplier network uses multi-factor authentication. The Supplier must ensure that any servers used to provide the service to Wincanton are not deployed on untrusted networks (network's outside your security perimeter, that are beyond The Suppliers administrative control e.g., internet-facing) without appropriate security controls. The Supplier hosting Wincanton's information (including sub-contractor) in a data centre or cloud must hold a valid ISO 27001and/or SOC 1 or 2 certification for security management (or certification(s) that demonstrate equivalent controls, supported by an independent auditor report).	If this principle is not implemented, external or internal networks could be subverted by attackers in order to gain access to the service or data within it.

Denial of Service Detection	The Supplier must maintain a capability to detect and protect against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The Supplier must ensure that Internet connected or external channels supporting services supplied to Wincanton must have adequate DoS protection to ensure availability.	If this principle is not implemented, Wincanton, its Customers and its Suppliers may be unable to prevent a denial of service attack from achieving its objective.
Remote Access	The Supplier must ensure following components are established for remote access: • Remote login access to the supplier network must be encrypted during data in transit and use multi-factor authentication. • Supplier must maintain records of individuals who have been asked to work remotely and the rationale for such requirement • The Supplier must ensure that end point used for connecting to Wincanton information systems remotely must be configured securely (e.g. patch level, status of anti-malware, etc.).	Remote access controls help to ensure unauthorized and insecure devices are not connected to the Wincanton environment remotely.
Security Log Management	The Supplier must ensure that there is an established and supporting audit and log management framework which confirms that key IT systems including applications, networking equipment, security devices and servers are set to log key events and logs must be centralised, appropriately secured and retained by the Supplier for a minimum period of 12 months. The Supplier will ensure key events are logged that have the potential to impact the confidentiality, integrity and availability of the Services to Wincanton and that may assist in the identification or investigation of material incidents and/or breaches of access rights occurring in relation to the Supplier Systems.	If this control is not implemented, suppliers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.
Malware Protection	The Supplier must have policies and procedures established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organisationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Malware protection solutions are vital for the protection of Wincanton's Information assets against Malicious code.
Endpoint Security	The Supplier must ensure that endpoints used to access the Wincanton network, or access/process Wincanton's data, are hardened to protect against attack and compromise. Endpoint security must include: • Disk encryption. • Disable all un-needed software/services/ports. • Disable administration rights access for local user. • Removable media / portable devices should be disabled by default and only enabled for legitimate business reasons. • Updated with the latest anti-virus signatures and security patches. · • Data Loss Prevention limited to no cut-copy-paste and print-screen of Wincanton data • By default, Printer access must be disabled. • Restricting the ability to access social networking sites, webmail services and sites with the ability to store information on the internet like google drive, Dropbox, iCloud.	If this control is not implemented, Wincanton and Supplier network and endpoints may be vulnerable to attack.

	- Prevent the sharing/ Transferring of Wincanton’s data should be disabled using instant messaging tools/ software. - Capability and processes to detect unauthorised software identified as malicious and prevent installation of unauthorised software. The Supplier must ensure they implement mobile device management (MDM) capabilities to securely control and manage mobile devices throughout the lifecycle that have access and/or contain classified Wincanton’s information, reducing the risk of data compromise. The Supplier must ensure mobile device remote lock and wipe capabilities are implemented to protect information in the event of a lost, stolen or compromised device. The Supplier must ensure the encryption of mobile device data (Wincanton Data).	
Data Leakage Prevention	The Supplier must have an established framework to ensure that protection against inappropriate data leakage is in place ensuring protection includes the following data leakage channels (but not limited to): - Unauthorised transfer of information outside the internal network/ supplier network - Email - Internet / Web Gateway (including online storage and webmail) - Loss or theft of Wincanton’s Information Assets on portable electronic media (including electronic Information on laptops, mobile devices, and portable media). - Unauthorised transfer of Information to portable media. - Insecure Information exchange with third parties (subcontractors). - Inappropriate printing or copying of Information.	Appropriate controls must be operated effectively in order to ensure that Wincanton’s information is restricted to those who should be allowed to access it (confidentiality), protected from unauthorised changes (integrity) and can be retrieved and presented when it is required (availability).
Data Protection	The Supplier will ensure appropriate Data Protection of Wincanton Information Assets, including but not limited to - Ensure viewing and use of sensitive information is controlled via access management capabilities to protect against exploitation of sensitive information. - Utilise data masking and obfuscation technologies to effectively protect sensitive data in use from inadvertent disclosure and/or malicious exploitation. The Supplier will ensure appropriate Data in transit protection, including but not limited to - Strong encryption to ensure data is protected while in transit. - Encryption of data in transit is typically achieved using Transport or Payload (Message or Selective Field) encryption. - Transport security protocols must be configured to prevent negotiation of weaker algorithms and/or shorter key lengths, when both end points support the stronger option. The Supplier will ensure appropriate Data Backup, including but not limited to	If these requirements are not implemented, it may result in Wincanton’s Sensitive Information being vulnerable to unauthorized modification, disclosure, access, damage, loss or destruction, which may result in legal and regulatory sanction, reputational damage, or loss / disruption of business

	• Ensuring Information is adequately backed up and recoverable in compliance with requirements agreed with Wincanton. • Ensuring that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services. • Ensuring that all Wincanton data is automatically backed up on a regular basis.	
Application Software Security	The Supplier must develop applications using secure coding practices and in a secure environment. Where the Supplier develops applications for use by Wincanton or its Customers, or which are used to support the service to Wincanton, Supplier must establish a Secure Development framework to prevent security breaches and to identify and remediate vulnerabilities in the code during the development process. The Supplier will ensure that application software security includes, but is not be limited to the following: • Ensuring secure coding standards are in place and adopted in line with Industry Best Practices to prevent security vulnerabilities and service interruptions which at the same time defends against possible well-known vulnerabilities. • Establishing secure coding practices appropriate to the programming language. • All development must be undertaken in a non-production environment • Maintain separate environments for production and non-production systems. • Developers should not have unmonitored access to production environments. • Segregation of duty for production and non-production environments. • Systems are developed in line with Secure Development best practice (e.g. OWASP). • Code should be securely stored and subject to Quality Assurance. • Code should be adequately protected from unauthorised modification once testing has been signed off and delivered into production. • Only use up-to-date and trusted third-party components for the software developed by the supplier. • Apply static and dynamic analysis tools to verify that secure coding practices are being adhered. • The Supplier must ensure that live data (including Personal Data) will not be used within non-production environments. • Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications). The Supplier must protect web applications by deploying web application firewalls (WAF) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall must be deployed.	Controls protecting application development helps to ensure that applications are secured at deployment.
Logical Access Management	Access to information must be restricted, and with due consideration of the need-to know, the least privilege and the segregation of duties principles. The Information Asset Owner is accountable for deciding who needs what access: • The need-to-know principle is that people should only have access to Information which they need to know in order to	Appropriate LAM controls help to ensure that Information Assets are protected from inappropriate usage. Appropriate controls must be operated

	perform their authorised duties. • The least privilege principle is that people should only have the minimum level of privilege necessary in order to perform their authorised duties. • The segregation of duties principle is that at least two individuals are responsible for the separate parts of any task in order to prevent error and fraud. Access management processes should be defined as per Industry Best Practices and include the following: • The Supplier should ensure that access management processes must be documented and apply to all IT Systems (which store or process Wincanton Information Assets), and when implemented they must provide appropriate controls for: Joiner /Mover/ Leaver/ Remote Access. • Controls must be in place for authorisation to ensure the process for granting, modifying and revoking access includes a level of authorisation commensurate with the privileges being granted, and in a timely fashion • All Privileged Access permissions must be reviewed at least annually, and adequate controls must be implemented for Privileged Access requirements.	effectively in order to ensure that Wincanton's information is restricted to those who should be allowed to access it (confidentiality), protected from unauthorised changes (integrity) and can be retrieved and presented when it is required (availability). If these requirements are not implemented, it may result in Wincanton's Sensitive Information being vulnerable to unauthorised modification, disclosure, access, damage, loss or destruction, which may result in legal and regulatory sanction, reputational damage, or loss / disruption of business.
Vulnerability Management	The Supplier must have policies and procedures established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organisationally-owned or managed applications, infrastructure network and system components to ensure the efficiency of implemented security controls. All security issues and vulnerabilities, which could have a material effect on Wincanton's' hosting infrastructure and/or web applications provided by the Supplier, that the Supplier has decided to risk accept must be communicated/ notified to Wincanton promptly and agreed in writing with Wincanton's IT Security Team.	If this control is not implemented, attackers could exploit vulnerabilities within systems to carry out Cyber-attacks against Wincanton, its Customers and Suppliers.
Patch Management	The Supplier must have policies and procedures established, and supporting business processes and technical measures implemented, to deploy security patches to managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. The Supplier must ensure that the latest security patches are applied to systems / assets / networks / applications in a timely manner ensuring that: • Supplier should test all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity. If a system cannot be patched, deploy appropriate countermeasures. • All key IT changes prior to implementation must be logged, tested and approved via an approved, robust change management process to prevent any service disruption or security breaches. • Supplier must ensure that patches are reflected in Production and DR environments.	If this control is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.

Threat Simulation, Penetration Testing and IT Security Assessment	The Supplier must engage with an independent qualified security provider to perform an IT security assessment / threat simulation covering IT infrastructure including disaster recovery site and web applications related to the service(s) that the Supplier provides to Wincanton. This must be undertaken at least annually to identify vulnerabilities that could be exploited to breach the confidentiality of Wincanton Data through Cyber Attacks. All vulnerabilities must be prioritised and tracked to resolution. The test must be undertaken in line with Industry Best Practices. For Supplier services related to Hosting infrastructure/ application on behalf of Wincanton, The Supplier must inform and agree on the scope of security assessment with Wincanton, in particular start and end date/times, to prevent disruption to key Wincanton activities. Any or all issues which are risk-accepted must be communicated and agreed with the Wincanton IT Security Team	If this control is not implemented, Suppliers may be unable to assess the Cyber threats they face and the appropriateness and strength of their defences. Wincanton information may be disclosed and / or loss of service may occur leading to legal and regulatory sanction, or reputational damage.
Cryptography	The Supplier must document the rationale for utilising cryptographic technology and review this to ensure that it is still fit for purpose. The Supplier must hold and maintain a documented set of cryptography lifecycle management procedures detailing the end to end processes for key management from generation, loading, distribution to destruction. The supplier must ensure all human managed events for keys and digital certificates, including the registration and generation of new keys and certificates, are approved at an appropriate level and a record of the approval retained. The supplier must ensure all certificates are procured from a set of approved and vetted Certificate Authorities (CA) which have revocation services and certificate management policies and must ensure Self Signed certificates are only utilised where technically unable to support a CA based solution and must have manual controls in place to ensure the integrity, authenticity of the keys and timely revocation and renewal is achieved. The supplier maintains a backup of all keys to prevent the service from being interrupted if the keys become corrupted or require restoration. Access to the back-ups are restricted to secure locations under split knowledge and dual control. Key Backups must have at least as strong cryptographic protection over them as the keys in use. The supplier maintains a complete and up-to-date inventory of cryptographic use in the services they provide to Wincanton that details all cryptographic keys, digital certificates, cryptography software and cryptographic hardware managed by the supplier to prevent damage in case of an incident. It is evidenced by signing of the inventory reviewed at least every quarter and provided Wincanton. The strength of the encryption deployed must be commensurate to the risk appetite, as it may have an operational or performance impact.	If this control is not implemented, appropriate physical and technical controls may not be in place leading to service delays or disruption or Cyber Security Breaches occurring.

Cloud Computing	The Supplier should be certified to ISO/IEC 27017 or 27001or SOC 1or 2 have established and supporting business processes and technical measures implemented to ensure that all use of Cloud technology is subject to appropriate security controls implemented.	If this control is not implemented inappropriately protected Wincanton data could be compromised, which may result in legal and regulatory sanction, or reputational damage.
Right of Inspection	The Supplier must allow Wincanton, upon Wincanton giving not less than ten (10) business days written notice, to conduct a security review of any site, system, technology or functional capability used by the Supplier or its Sub-contractors to develop, test, enhance, maintain or operate the Supplier systems used in the Services, in order to review the Supplier's compliance with its obligations. The Supplier must allow Wincanton to carry out an assessment on at least an annual basis or immediately after a security incident. Any non-compliance of controls identified by Wincanton during an inspection must be risk assessed by Wincanton and Wincanton should specify a remediation timeframe. The Supplier should then complete any required remediation within that timeframe. The Supplier must provide all assistance reasonably requested by Wincanton in relation to any inspection and documentation submitted during inspection needs to be completed and return back to Wincanton.	If not agreed, Suppliers will be unable to provide full assurance of compliance to these security obligations.