Supplier Control Obligations

Information Security

(STAN-037)

OVERVIEW

The purpose of this document is to set clear expectations for our external suppliers with regard to information and cyber security.

The requirements contained within this document are shared with potential suppliers at the start of the tender process and during the contracting phase. This document forms part of our contractual agreement with suppliers.

Principality expect suppliers to adhere to these obligations.

Principality do conduct ongoing assurance activity to verify compliance with the relevant obligations.

The obligations apply to all suppliers. The suppliers that store, process or transmit data classified as 'Restricted' by Principality have additional obligations. Please refer to Appendix A – STAN-035 Principality Data Classification Scheme.

Please note the data classification scheme is included for informational purposes only. Principality will ensure the classification level of data that falls within the scope of supplier engagements is defined at the start of the tender process.

Control	Control Description	Why?
Roles and Responsibilities	The Suppliers management shall ensure that roles and responsibilities for Information and Cyber Security are defined, assigned and communicated. This should be done in accordance with Information Security Policies. These roles and responsibilities must be reviewed after any change in the Suppliers business or operating model. Key roles must include a senior manager, accountable for Information and Cyber Security. It is the Suppliers responsibility to ensure that their employees are familiar and comply with the control requirements of this standard.	Clearly defined roles and responsibilities supports the implementation of External Suppliers Control Obligations.
Risk Management Framework	The Supplier must establish a risk management framework that includes security which effectively evaluates, monitors and mitigates security risks across the Supplier business. The risk management framework should include but not be limited to the following: • Formal risk assessment should be performed at least annually to determine the likelihood and impact associated with identified security risks • Appropriate risk treatment options are selected based on risk assessment findings • Risk treatment plans are documented • Risk is managed to a defined and acceptable level • Risk owners are identified who are accountable for the management of identified risks ***Additional requirements that apply to Suppliers who:*** • ***process, store or transmit RESTRICTED data*** The Supplier must have an established a consistent industry standard framework for Information Security in accordance with recognised industry standards (current industry standards include NIST, ISO/IEC 27001, CIS).	Identifying potential threats and how they may impact a business is key to ensuring that adequate safeguards and countermeasures are in place to protect the confidentially, integrity and availability of information assets.

	The Security framework must be developed, documented, approved, and implemented which includes administrative, organisational, technical, and physical safeguards to protect assets and data from unauthorised loss, misuse, access, disclosure, alteration, and destruction.	
Human Resource Security	Background verification checks should be carried out on all Supplier personnel prior to employment in accordance with relevant laws and regulations (These checks should be proportionate to the business requirements). Supplier employee contracts must reflect the organisations policies for Information Security in addition to other clauses based on their role within the Suppliers organisation (e.g. Non-Disclosure Agreements based on Classification of Information to be accessed). Suppliers must have a process in place to control logical and physical access for employees who have their employment terminated or changed. The Supplier must implement measures to mitigate the risk of insider threats, where legitimate access is misused for unauthorised purposes.	Information Security should be reflected in Supplier employee contracts and HR process.
Training and Awareness	All employees of the Supplier should receive appropriate awareness and complete training within one month of joining the Supplier and then updated within an appropriate time frame (annually at least) in regards to Information Security. A record of all employee training must be retained. The training and awareness material should include clear expectations for Supplier employees in terms of: • organisational processes • procedures • policies It should also raise awareness of current and evolving threats by providing advice and guidance. The training should include but not be limited to the following: • Social engineering • Phishing • Setting and managing strong passphrases • Secure browsing	Reduces the risk of an Information Security Incident as well as supporting all the controls within this standard. Ensures Supplier personnel understand their Information Security roles and responsibilities.

	• Importance and use of MFA • Reporting processes (e.g. suspicious emails) ***Additional requirements that apply to Suppliers who:*** • ***process, store or transmit RESTRICTED data*** The Supplier must have an established security training and awareness program for all employees and users of the Suppliers systems. The level of training and awareness must be commensurate to the roles being undertaken. Progress and performance of all employees must be recorded and tracked in an appropriate management platform. The Supplier must identify high-risk groups, such as system administrators and other privileged users. These groups should receive enhanced training and awareness materials aligned to their roles and responsibilities.	
Approved Usage	The Supplier must produce, publish and communicate Acceptable Use Requirements informing Supplier employees of their responsibilities. The following areas must be considered (Use of): • Internet Usage • Corporate Email • Social Media • Instant Messaging • IT Equipment provided by Supplier • Personal IT Equipment (BYOD) • Information classification & handling • Data Leakage Appropriate steps must be taken to ensure compliance to the above.	Acceptable Use Requirements help underpin the control environment protecting information assets.
Data Classification	The Supplier must ensure an appropriate information classification and handling scheme is implemented, based on recognised industry standards which includes but is not limited to the following: • Assigning Principality data the correct information labelling classification	The classification of information/data determines its level of sensitivity and criticality to Principality.

	• Handling, storing and disposing Principality data appropriately, in line with its assigned level of classification • The Supplier will ensure Principality handling, storage and disposal requirements map accurately to an internal scheme which will provide the equivalent, or greater protection, if opting to label Principality data with the Suppliers own information labelling scheme • Ensuring all Supplier employees are aware of the relevant information handling, storage and disposal requirements The Supplier must refer to the Principality data classification scheme (Appendix A).	
Physical Security	The Supplier must have physical controls in place to prevent unauthorised physical access, damage and interference to the information or services that the Supplier provides to Principality wherever they are stored or processed. Security perimeters and visitor access procedures should be adequate to the security requirements of the assets within their perimeter based on risk assessments.	This helps to ensure integrity within the Supplier organisations physical premises and that their information and information processing facilities are secure.
Firewalls	The Supplier must ensure that only safe and necessary network services can be accessed from the internet. The Supplier must adequately protect their network services utilising firewalls or equivalent network devices. All devices should be protected by a correctly configured boundary firewall, software firewall (or equivalent network device). All firewalls (or equivalent network devices) must be implemented following good industry practice and based on risk exposure and business need. The implementation must consider: • changing any default administrative passwords or disable remote administrative access entirely • controlling access to the administrative interface (used to manage firewall configuration) from the Internet, • Blocking unauthenticated inbound connections by default • Approval process for inbound firewall rules • remove or disable unnecessary firewall rules at the point they are no longer needed	All devices run network services, which create some form of communication with other devices and services. By restricting access to these services your exposure to attacks is reduced.

	• use of a software firewall for devices which are used on untrusted networks, such as public WiFi hotspots	
Secure Configuration	The Supplier must ensure that computer and network devices have been configured properly to reduce the level of inherent vulnerabilities and to provide only the services required for operational business requirements. The Supplier must be active in its management of end user devices, servers, operating systems and other network devices and follow good industry practices. The Supplier must: • remove and disable unnecessary user accounts • change any default or guessable account passwords • remove or disable unnecessary software (including applications, system utilities and network services) • disable any auto-run feature which allows file execution without user authorisation • ensure authentication of users before allowing access to organisational data or services • ensure appropriate device locking controls that are designed to be resistant to brute-force attacks ***Additional requirements that apply to Suppliers who:*** • ***process, store or transmit RESTRICTED data*** The Supplier must have an established framework to ensure that all configurable systems/networking equipment and end user devices are securely configured in accordance with recognised industry standards (e.g. NIST, CIS). The framework should include but not be limited to the following: • Systems, networking equipment and end user devices are configured to function in accordance with recognised industry configuration standards • Compliance monitoring solutions ensure that devices which do not adhere to baseline security standards are identified and rectified	Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points. Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.
Cloud Security	The Supplier must ensure that any cloud service providers are certified to a recognised industry standard.	Unless robust controls are used to protect data contained in

	The Supplier is responsible for ensuring appropriate data security controls are implemented to protect any Principality information assets within the cloud. This includes but is not limited to: • configuration of the cloud environment should address known issues that jeopardise the confidentiality, integrity, availability and accessibility of information in cloud services • all access to service interfaces should be constrained to authenticated and authorised individuals • multi-factor authentication is implemented for all users • service generates adequate audit events to support effective identification of suspicious activity • protection of data in-transit, in-use and at-rest • If using multi-tenancy cloud services sufficient data segregation to ensure data is isolated and not accessible to other tenants The Supplier must confirm they can integrate with the Society's Single Sign-On ('SSO') / Multifactor Authentication application prior to any contract commencement and maintain this functionality throughout the contract. All Cloud services must be accessed **only** through the Society's SSO / MFA application. Cloud service exemptions to this rule can only be provided by the Head of IT.	cloud services Principality data could be compromised.
User Access Control	The Supplier must ensure access to information is restricted by requiring all user accounts to authenticate before accessing information or services. Only authorised individuals will be provided user accounts, and they are granted only as much access as they need to perform their role. The Supplier must: • have a user account creation and approval process • authenticate users before granting access to applications or devices, using unique credentials • remove or disable user accounts when no longer required (e.g. when a user leaves the organisation) • implement MFA where individuals are accessing environments which contain Principality data	Every active user account in your organisation facilitates access to devices and applications, and to sensitive business information.

	• authentication to cloud services must always use MFA • use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks) • remove or disable special access privileges when no longer required • all administration accounts (privileged accounts) must always use MFA • implement mover and leaver controls to ensure access is revoked when no longer required	
Authentication Policy	Password-based authentication Where this is done using a password, the following protections should be used: • Passwords are protected against brute-force attacks using an industry recognised solution • Technical controls are used to manage the quality of passwords in line with recognised industry standards. • There is an established process to change passwords promptly if the applicant knows or suspects the password or account has been compromised. Multi-Factor Authentication (MFA) As well as providing extra protection for passwords, MFA should always be used to provide additional protection to administrative accounts, and accounts that are accessible from the internet. The type of additional factor should balance the risks of confidentiality and availability and be supported by a recognised industry standard or technical authority (such as NCSC). Additional factors may include: • A managed/enterprise device • An app on a trusted device • A physical separate token • A known or trusted account	The use of strong passphrases and multi-factor authentication significantly reduces the likelihood of account compromises.

Access Control	***Additional requirements that apply to Suppliers who:*** • ***process, store or transmit RESTRICTED data*** The Supplier must provision access based on the principles of 'need to know', 'least privilege' and 'segregation of duties'. The Supplier must appoint an owner who is responsible for approving, modifying, revoking and defining the level and period of access to RESTRICTED data. This process must take into account the following: • employees should only be given access in order to perform their authorised duties • employees must only have the minimum level of access necessary in order to perform their authorised duties • any task that could lead to significant disruption or damage must require at least two individuals responsible for the separate parts of the task (e.g. request and approval) • access and permissions are reviewed at least every 12 months The Supplier must document all access management decisions and processes. The Supplier must ensure all access to RESTRICTED data is logged and can be associated to a single individual.	By ensuring that only authorised individuals have user accounts, and that they are granted only as much access as they need to perform their role, you reduce the risk of information being stolen or damaged.
Malware Protection	The Supplier must restrict execution of known malware and untrusted software to prevent harmful code from causing damage or accessing data. The Supplier must implement a malware protection programme. The Supplier must ensure: • The software (and all associated malware signature files) are kept up to date. • The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder. • The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself). • The supplier must prevent connections to malicious websites on the Internet— unless there is a clear, documented business need and the Supplier understands and accepts the associated risk.	If a system is infected with malware, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere.

	Where anti-malware software is not utilised alternative protection mechanisms must be implemented: • Application allow-listing – the supplier must ensure only approved applications, restricted by code signing are allowed to execute on devices • Application sandboxing – the supplier must ensure all unknown executables are run within a 'sandbox' that prevents access to other resources	
Patch Management	The Supplier must ensure that devices and software are not vulnerable to known security issues for which fixes are available. The Supplier must keep all its software up to date. All software must be: • licensed and supported • removed from devices when it becomes un-supported or effective risk treatment is implemented, such as preventing all connections to / from the internet • have automatic updates enabled where possible The Supplier must update its software as soon as is practically possible, including applying any manual configuration changes required to make the update effective, within a maximum of 30 days of an update being released ○ The supplier must assess the risk of any updates which addresses any vulnerabilities described by the vendor as 'critical' or 'high' to establish if 30 days is an acceptable and reasonable period of exposure	Any device that runs software can contain security flaws, known as 'vulnerabilities' which can exploited.
Vulnerability Management	The Supplier must have policies and procedures established, supporting processes, organisational and technical measures implemented, for effective monitoring, timely detection, remediation of vulnerabilities within Supplier owned or managed applications, infrastructure network and system components. ***Additional requirements that apply to Suppliers who:*** • ***process, store or transmit RESTRICTED data*** The Supplier must have an established vulnerability management framework which includes but is not limited to the following: • appropriate tools and infrastructure for vulnerability scanning that are operated in-house or by a managed service provider	Vulnerabilities are regularly discovered in all sorts of software. Once discovered, malicious individuals or groups move quickly to misuse (or 'exploit') vulnerabilities to attack computers and networks in organisations with these weaknesses.

	• vulnerability scanning is conducted on a regular basis commensurate with the risk of the asset class • criteria that prioritises the remediation of discovered vulnerabilities • remediation validation process to ensure discovered vulnerabilities have been remediated The Supplier must notify Principality of all vulnerabilities that the Supplier has decided to risk accept which could have a significant effect on Principality.	
Data Loss Prevention	The Supplier must have appropriate protection mechanisms in place to mitigate data loss. Suppliers that handle Principality data must ensure our information assets are monitored for inappropriate data leakage through the following channels: • unauthorised transfer of information outside the supplier network via common egress channels • unauthorised transfer of information to portable media • inappropriate printing of information • loss or theft of information held on portable ***Additional requirements that apply to Suppliers who:*** • ***process, store or transmit RESTRICTED data*** The Supplier must prevent RESRTICTED data being transferred via: • email • internet gateways (including online storage) • USB storage devices • external hard drives • subcontractors Should there be a business need to do so the Supplier must obtain the express permission of Principality.	Data leakage can occur from a variety of sources; email, internet, printers, hard disks and waste paper being just a few.
Data Security	The Supplier must maintain an inventory of all Principality data stored, processed and transmitted by the Supplier.	The use of robust data security controls helps prevent the unauthorised disclosure,

	The Supplier will ensure the following organisational and technical measures are implemented where Principality data is stored, processed and transmitted which include but are not limited to the following:
	
	• Data-at-rest
	  ○ appropriate controls, commensurate with the criticality and sensitivity of the data, are implemented to protect from unauthorised access.
	
	• Data-in-transit
	  ○ transport encryption mechanisms must be used to ensure the transport layer, payload or both protect data in transit. The utilised mechanism must be in line with supported cryptographic solutions (protocols, algorithms, ciphers, keys) recognised by a competent cryptographic authority.
	
	• Data-in-use
	  ○ Access to information is limited and controlled based on the principles of 'need to know', 'least privilege' and 'separation of duties'. The Supplier must evaluate who has a need to read, modify or delete data ensuring it is restricted by default.
	
	• Database-data store monitoring
	  ○ Monitor and log access and activity to data stores such as databases to identify malicious activity
	
	• Data backups
	  ○ Data in backup media whether physical or virtual should be adequately protected by physical security or encryption.
	
	• Non-production environments
	  ○ The Supplier will ensure development and test environments are separate from the production environment.
	  ○ The Supplier will ensure Principality data is not used in development and test environments without the express permission of Principality
		modification, damage, loss or destruction of Principality data.

	Additional requirements that apply to Suppliers who:
	• ***process, store or transmit RESTRICTED data***
	
	The Supplier must ensure all RESTRICTED data is classified and tagged.
	
	• Data-at-rest
	  ○ At a minimum, RESTRICTED data must be encrypted at rest
	
	• Data-in-use
	  ○ The Supplier should consider utilising data masking and obfuscation technologies to protect sensitive data in use	

Cryptography	The Supplier must review and assess the cryptographic technology and algorithms it uses to ensure that it is still fit for purpose. The strength of the encryption deployed must be commensurate to the risk. Where encryption is utilised the Supplier must ensure that any encryption keys or other forms of protection are kept secure. The Supplier must: • document and implement procedures to protect keys used to secure stored data • restrict access to cryptographic keys • store encryption keys securely using a recognised industry standard approach (such as with a secure cryptographic device) • only generate cryptographically strong encryption keys • secure the distribution and storage of keys • formal process for retiring and destroying the keys	Up to date and appropriate encryption protection and algorithms ensures the continued protection of Principality Information Assets.
Security Control Assessment and Assurance	The Supplier must have a framework which defines the objectives of the controls which protect the Suppliers internal and external IT infrastructure, including its use of Cloud Service Providers related to the services the Supplier provides to Principality.	

	The Supplier must have a framework which assesses the effectiveness of the controls which protect the Suppliers internal and external IT infrastructure, including its use of Cloud Service Providers related to the service the Supplier provides to Principality. The Supplier must ensure any applications or services which are available via the internet which process, store or transmit Principality data are assessed by an independent qualified security assessor on a regular basis, at least annually. ***Additional requirements that apply to Suppliers who:*** • ***process, store or transmit RESTRICTED data*** The Supplier must engage with an independent CREST accredited security company to perform a security assessment covering its internal and external IT infrastructure including any cloud services, applications related to the services that the Supplier provides to Principality. This must be undertaken at least annually to identify vulnerabilities that could be exploited through cyber-attacks. All findings should be evaluated, based on risk, prioritised and tracked to resolution.	
Incident Management	The Supplier must have an incident management framework that effectively identifies, validates, evaluates, contains, escalates and remediates security incidents. The Supplier must test incident response teams and processes, at least annually, to demonstrate they are able to respond to information security incidents. The Supplier incident response processes must include: • notification requirements if an incident could impact Principality data or services provided • points of contact who will liaise with Principality in the event of an incident • incident severity classification based on impact and likely consequences to Principality • escalation pathways to appropriate stakeholders and accountable individuals	An incident response framework helps to ensure that incidents are quickly contained to limit the disruption and damage an incident could cause.

	The Supplier will inform Principality upon becoming aware of any incident that impacts or is suspected might impact Principality no later than 2 hours from the time the Supplier becomes aware of the security incident. In addition to the initial notification, the Supplier will provide a written update to Principality within 24 hours of the notification of any security incident which impacts Principality. The update must include the following detail: • timeline of events • summary of the incident • impact and likely consequences • action taken • incident status (is it ongoing or contained) • planned action • date/time of next update In the event Principality is significantly impacted as a result of a security incident the Supplier will provide a full and detailed investigation report detailing the what, when and how of the incident no later than 5 working days of the Supplier receiving it.	

Appendix A: Principality Data Classification – STAN-035

Classification	Definition	Access	High Level Examples
Secret	Information that is highly sensitive. Its unauthorised disclosure, alteration or destruction could cause a serious and likely level of risk resulting in severe adverse effects to the Society, Customers or Colleagues.	Access is strictly limited to a small number of named individuals only.	• Authentication verification data • Cryptographic materials • Source code • Highly sensitive infrastructure data • Highly sensitive investigation data

Restricted	Information that is high risk. Its unauthorised disclosure, alteration or destruction could cause a high level of risk resulting in substantial detriment to the Society, customers or colleagues.	Access is controlled and restricted internally, usually to specific roles and/or groups. When shared externally there must be business justification, permission from the data originator/owner, a clear 'need to know' for the recipient.	• High risk personal data
			  ○ Special category data
			  ○ Criminal conviction and offence
			  ○ Personal data relating to children
			  ○ Significant unique identifiers (passport/NI number etc)
			• Sensitive business management information
			• HR/Employee data
			• Transactional payment system data

Internal	Information that is needed to conduct day-to-day business. Its unauthorised disclosure, alteration or destruction could result in a low to moderate level of risk resulting in minor to significant detriment to the Society, customer or colleagues.	Access is limited to internal distribution, including authorised third party providers, to those that have a valid business justification to access or receive it.	• Personal data (not included in Restricted)
			• Routine business management information
			  ○ Policies, procedures, manuals, templates
			  ○ Internal communications
			  ○ Reports, MI, meeting packs/minutes
			• Customer/Client service and/or marketing communications

Public	Information intended for general external distribution, already in the public domain or would have no negative impact to the Society if it were to be distributed.	Access is unrestricted and may be viewed by anyone inside or outside the organisation.	• Marketing materials • Job advertisements/ recruitment data • Published financial reports • Published press releases