TORBAY COUNCIL CLOUD INFORMATION SECURITY QUESTIONNAIRE

Based on NCSC's Guidance "Implementing the Cloud Security Principles", 17 November 2018

https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

CHANGE LOG

VERSION	CHANGE	DATE	AUTHOR
1.0	Created	07/03/2016	Gavin Dunphy

Item	Principle	Supplier's Response
1	**Data in transit protection** Council data transiting networks should be adequately protected against tampering (integrity) and eavesdropping (confidentiality). This should be achieved via a combination of: - network protection (denying your attacker access to intercept data) - encryption (denying your attacker the ability to read data) The Service should be sufficiently confident that: - Data in transit is protected between ALL end user devices and the Cloud Service Data in transit is protected internally within the Cloud service - Data in transit is protected between the Cloud Service and other services (e.g. where APIs are exposed) -	
2	**Asset protections and resilience** User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	
	Physical Location and Legal Jurisdiction The locations at which data is stored, processed and managed from, must be identified so that the Service can understand the legal circumstances in which the data could be accessed without our consent. The Service needs to understand how data handling controls within the Cloud Service offering are enforced, relative to UK legislation. Inappropriate protection of the data could result in legal and	

	regulatory sanction or reputational damage.	
	Data centre security The locations used to provide Cloud Services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data. The Service should be confident that the physical security measures employed by the Cloud Service provider are sufficient for their intended use of the Cloud Service. **Data at rest protection** The data should be protected when stored on any type of media or storage within a Cloud Service to ensure that it is not accessible by local unauthorised parties. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media. The Service should have sufficient confidence that storage media containing their data is protected from unauthorised access.	

	Data sanitisation The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to the services data. Inadequate sanitisation of data could result in: - The Service data being retained by the Cloud Service provider indefinitely - The Service data being accessible to other users of the Cloud Service as resources are reused - The Service data being lost or disclosed on discarded, lost or stolen media. The Service should be sufficiently confident that: - Their data is erased when resources are moved or re-provisioned, when they leave the provider or when they request it to be erased Storage media which has held Service data is sanitised or securely destroyed at the end of its life **Equipment disposal** Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way that does not compromise the security of the Cloud Service or the data stored in the Cloud Service. The Service should be sufficiently confident that: - All equipment potentially containing service data, credentials, or configuration information for the Cloud Service is identified at the end of its life (or prior to being recycled). - Any components containing sensitive data are sanitised, removed or destroyed as appropriate. - Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker	

	Physical resilience and availability Cloud Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A Cloud Service without guarantees of availability may become unavailable, potentially for prolonged periods, with attendant business impacts. The Service should be sufficiently confident that the availability commitments of the Cloud Service provider, including their ability to recover from outages, meets their business needs.	

3	**Separation between users** Separation between different users of the Cloud Service prevents one malicious or compromised user from affecting the service or data of another. Some of the important characteristics which affect the strength and implementation of the separation controls are: - the service model (e.g. IaaS, PaaS, SaaS) of the cloud service - the deployment model (e.g. public, private or community cloud) of the Cloud Service - the level of assurance available in the implementation of separation controls The Service should - understand the types of user they share the Cloud Service or platform with - have confidence that the Cloud Service provides sufficient separation of their data and service from other users of the Cloud Service - have confidence that their management of the Cloud Service is kept separate from other users	
4	**Governance Framework** The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the Cloud Service and information within it. When procuring a Cloud Service, ensure that the supplier has a suitable security governance framework in place. Regardless of any technical controls deployed by the supplier, controls will be fundamentally undermined if operating outside an effective risk management and governance regime. A governance framework will ensure	

	that procedure, personnel, physical and technical controls remain effective through the lifetime of the Cloud Service, in response to changes in the Cloud Service, and changes in threat and technology developments. Good governance will typically provide: - A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title Chief Security Officer, Chief Information Officer or Chief Technical Officer. - A documented framework for security governance, with policies governing key aspects of information security relating to the service. - Security and information security as part of the service provider's financial and operational risk reporting mechanisms. - Processes to identify and ensure compliance with applicable legal and regulatory requirements relating to the Cloud Service. The Service should have sufficient confidence that the governance framework and processes in place for the Cloud Service are appropriate for their intended use.	
5	**Operational Security** The service provider should have processes and procedures in place to ensure the operational security of the Cloud Service. The Cloud Service will need to be operated and managed securely in order to impede, detect or prevent attacks against it. The aspects to consider comprise: - Configuration and Change management - ensuring that changes to the system do not	

	unexpectedly alter security properties and have been properly tested and authorised - - Vulnerability Management - ensuring that security issues in constituent components are identified and mitigated - Protective monitoring - taking measures to detect attacks and unauthorised activity on the service - - Incident management - ensuring the service can respond to incidents and recover a secure available service	
6	**Personnel security** Service provider staff should be subject to personnel security screening and security education for their role. Personnel within a cloud service provider with access to user data and systems need to be trustworthy. Service providers need to make clear how they screen and manage personnel within any privileged roles. Personnel in those roles should understand their responsibilities and receive regular security training. More thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise of user data by service provider personnel. The Service should be content with the level of security screening conducted on service provider staff with access to their information or with ability to affect their Cloud Service.	-
7	**Secure Development** Cloud Services should be designed and developed to identify and mitigate threats to their security. Cloud Services which are not designed securely may be vulnerable to security issues which could compromise	

	user data, cause loss of service or enable other malicious activity. The Service should be sufficiently confident that: New and evolving threats are reviewed and the service improved in line with them. Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment. Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.	
8	**Supply Chain Security** The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the Cloud Service claims to implement. Cloud services often rely upon third party products and services. Those third parties can have an impact on the overall security of the Cloud Services. If this principle is not implemented then it is possible that supply chain compromise can undermine the security of the Cloud Service and affect the implementation of other security principles. The Service understands and accepts: - How their information is shared with, or accessible by, third party suppliers and their supply chains. - How the service provider's procurement processes place security requirements on third party suppliers and delivery partners. - How the service provider manages security risks from third party suppliers and delivery partners. - How the service provider manages the conformance of their suppliers with security requirements.	

	- How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.	
9	**Secure user management** Users should be provided with the tools required to help them securely manage their service. Management interfaces and procedures are a vital security barrier in preventing unauthorised people accessing and altering users' resources, applications and data. The aspects to consider comprise: Authentication of users to management interfaces and within support channels In order to maintain a secure service, users need to be securely authenticated before being allowed to perform management activities, report faults or request changes to the Cloud Service. These activities may be conducted through a service management web portal, or through other support channels (such as telephone or email) and are likely to facilitate functions such as provisioning new service elements, managing user accounts and managing user data. It is important that service providers ensure any management requests which could have a security impact are performed over secure and authenticated channels. If users are not strongly authenticated then an attacker posing as them could perform privileged actions undermining the security of their service or data. The Service: Has sufficient confidence that only authorised individuals from the user organisation are able to authenticate to and access management interfaces for the service (Principle 10 should be used assess the risks of different approaches to meet this objective). Has sufficient confidence that only authorised individuals from the user organisation are able to perform actions affecting the user's service through support channels.	

	<u>Separation and access control within management interfaces</u> Many cloud services are managed via web applications or APIs. These interfaces are a key part of the Cloud Service's security. If Services are not adequately separated within management interfaces then one user may be able to affect the service, or modify data belonging to another. Users' privileged administrative accounts are likely to have access to large volumes of data. Constraining the permissions required by individual users to those absolutely necessary can help to limit the damage that could be caused by a malicious user, compromised credentials or device. Role-based access control provides a mechanism to achieve this. It is likely to be a particularly important capability for users managing larger deployments. Exposing management interfaces to less accessible networks (e.g. community rather than public networks) makes it more difficult for attackers to reach and attack them, as they would first need to gain access to the systems of one of the users or networks. The Service: - Has sufficient confidence that other users cannot access, modify or otherwise affect their service management. - Can manage the risks of their own privileged access, e.g. through 'principle of least privilege', providing the ability to constrain permissions given to user administrators. - Understands how management interfaces are protected and what functionality is available via those interfaces.	
10	**Identity and authentication** User and service provider access to all service interfaces should be constrained to authenticated and authorised individuals.	

	All cloud services will have some requirement to identify and authenticate users wishing to access service interfaces. Weak authentication or access control may allow unauthorised changes to a user's service, theft or modification of data, or denial of service. It is also important that authentication occurs over secure channels. Use of insecure channels such as email, HTTP or telephone can be more vulnerable to interception or social engineering attacks. The Service should have sufficient confidence that identity and authentication controls ensure users are authorised to access specific interfaces.	
11	**External interface protection** All external or less trusted interfaces of the Cloud Service should be identified and have appropriate protections to defend against attacks through them. If an interface is exposed to users or outsiders and it is not sufficiently robust, then it could be subverted by attackers in order to gain access to the Cloud Service or data within it. If the interfaces exposed include private interfaces (such as management interfaces) then the impact may be more significant. Users can use different models to connect to cloud services which expose their enterprise systems to varying levels of risk. The Service should; - understand how to safely connect to the Cloud Service whilst minimising risk to the user's systems. - understand what physical and logical interfaces their information is available from. - have sufficient confidence that protections are in place to control access to their data.	

	- have sufficient confidence that the Cloud Service can determine the identity of connecting users and services to an appropriate level for the data or function being accessed.	
12	**Secure Service administration** The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. The security of a cloud service is closely tied to the security of the service provider's administration systems. Access to service administration systems gives an attacker high levels of privilege and the ability to affect the security of the service. Therefore the design, implementation and management of administration systems should reflect their higher value to an attacker. A service administration network is a specialised form of enterprise network. There are a wide range of options for how this can be designed, delivered, managed and secured. It is expected that standard enterprise good practice be followed in the design and operation of these systems, but at a level reflecting their higher value. The service management systems are likely to have the most privileged access to the internals of the service. Compromise of them would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. If the service management model is not known, then it should be assumed that the high risk 'direct service management' model described below is used. The Service should have sufficient confidence that the technical approach the service provider uses to manage the cloud service does not put their data or service at risk.	

13	**Audit information provision to users** Users should be provided with the audit records they need to monitor access to their service and the data held within it. The type of audit information available to users will have a direct impact on their ability to detect and respond to inappropriate or malicious usage of their service or data within reasonable timescales. The Service needs to be: Aware of the audit information that will be provided to them, how and when it will be made available to them, the format of the data, and the retention period associated with it. Confident that the audit information available will allow them to meet their needs for investigating misuse or incidents.	
14	**Secure use of the service by the Service** The Service has certain responsibilities when using a Cloud Service in order for their use of it to remain secure, and for their data to be adequately protected. The security of cloud services and the data held within them can be undermined by poor use of the service by users. The extent of the responsibility on the user for secure use of the service will vary depending on the deployment models of the cloud service, specific features of an individual service and the scenario in which the users intend to the use the service. **End user devices used to access the service** As well as risks to the cloud service and user applications and data within it, users should consider the risks relating to their enterprise networks and end user devices used to access the service. Depending on how	

	the user is using the cloud service, it may be accessible to a range of end user populations and devices. For some applications it may be appropriate (indeed required) to allow citizen owned devices to connect to the service via a public web interface. However users from the user's organisation (e.g. case workers in a government department accessing citizen data) may require the use of enterprise-issued and managed devices with an appropriate configuration to provide sufficient security. - The user understands any service configuration options available to them and the security implications of choices they make. - The user understands the security requirements on their processes, uses, and infrastructure related to the use of the service. - The user can educate those administrating and using the service in how to use it safely and securely.	