TORBAY COUNCIL CLOUD INFORMATION SECURITY QUESTIONNAIRE

Based on NCSC's Guidance "Implementing the Cloud Security Principles", Version 2.0

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
2.0	Updated to correspond with NCSC website	09/06/2022	Pauline Godfrey

Item	Principle	Supplier's Response
1	**Data in transit protection** Customers' data transiting networks should be adequately protected against tampering and eavesdropping. This should be achieved via a combination of: - Encryption (denying an attacker the ability to read or modify data) - Network protection (denying an attacker the ability to intercept data - Authentication (denying an attacker the ability to impersonate the service) *How can the Council be confident that:* - *Data in transit is protected between ALL end user devices and the Cloud Service?* - *Data in transit is protected internally within the components of the Cloud service?* - *Data in transit is protected between the Cloud Service and other external services (e.g. where APIs are exposed)?*	
2	**Asset protection and resilience** Customers' data, and the assets storing or processing it, should be adequately protected against physical tampering, loss, damage or seizure.	
2.1	**Physical location and legal jurisdiction** *How can the Council be confident that it knows where its data is, and who can access it, in terms of:* - *In which countries data will be stored, processed and managed?* - *Which legal jurisdiction(s) data will be subject to, and whether this is acceptable to the Council?* - *The rights that you/the Cloud service provider will have to access and use Council data?*	

	- *The legal circumstances under which Council data could be accessed without consent, and how this affects the Council's compliance with UK legislation?* *This should include derivatives of Council data, such as verbose logs and machine learning models, unless sensitive aspects have been excluded or removed.*	
2.2	**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. *How can the Council be confident that the physical security measures employed by the Cloud Service provider are sufficient for the Council's intended use of the Cloud Service?* *Details of any standards the Cloud Service has been certified against in this area should be provided.*	
2.3	**Data encryption** Customers' data should be adequately protected from unauthorised access by parties with physical access to infrastructure, when considered alongside data at rest protections provided by encryption. Cloud service providers should encrypt all customer data at rest (preferably by default), including any metadata derived from that data. An appropriate encryption algorithm and mode should be used, which provide both confidentiality (to prevent unauthorised reading of the data) and integrity (to prevent un-noticed tampering of the encrypted data). *How can you demonstrate this?*	
2.4	**Data sanitisation and equipment disposal** The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to customers' data. Inadequate sanitisation of data could result in: - Council data being retained by the Cloud Service provider indefinitely.	

	- Council data being accessible to other users of the Cloud Service as resources are reused. - Council data being lost or disclosed on discarded, lost or stolen media. *How can the Council be confident that:* - *Council data is erased when resources are moved or re-provisioned, or when the Council requests it to be erased?* - *Storage media which has held Council data is sanitised or securely destroyed at the end of its life?* *The Cloud service provider should supply information on the processes and techniques used to sanitise equipment before disposal, referring to any certification held in this area.*	
2.5	**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. *How can the Council be confident that:* - *The availability commitments of the Cloud service provider, including the ability to recover from outages, meets the Council's business needs?* - *It understands whether the Cloud service provider's resilience processes have any implications for data residency?* - *The Council can protect its data from ransomware attacks?*	
3	**Separation between customers** Effective separation techniques ensure that one customer's service can't access or affect the service (or data) of another. *How can the Council be confident that:* - *It can control who can access Council data?* - *The Cloud service is robust enough to defend against another customer having malicious code in the Council's instance of the service?*	

	Describe how security separation has been implemented within the Cloud service, including security boundaries in: - *Compute (such as containerisation, Functions-as-a-Service, and IaaS)* - *Storage* - *Data flows and networking* *Where a SaaS or PaaS service is built on top of other PaaS or IaaS services (such as in a third-party cloud), the service provider should clarify which separation properties are inherited from the underlying components and infrastructure.*	
4	**Governance framework** A governance framework is vital to co-ordinate and direct the management of the Cloud service. The governance framework and processes in place for the Cloud Service should be appropriate for its intended use. *Describe the governance practices employed by the Cloud Service provider, including :* - *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 and risk management, with policies governing key aspects of information security relevant to the service.* - *Security and information security being part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board will be kept informed of security and information risk.* - *Processes to identify and ensure compliance with applicable legal and regulatory requirements relating to the Cloud Service.*	
5	**Operational security** Cloud Services must be operated and managed securely in order to impede, detect or prevent attacks.	
5.1	**Vulnerability management** Cloud Service providers should have a vulnerability management process in place to identify, triage and mitigate vulnerabilities in the component of the service they are responsible for.	

	How can the Council be confident that: - *It knows (and approves of), the service provider's timescales for deploying security updates and other mitigations?* - *The provider takes responsibility for applying security updates to all software and hardware, including where they rely on external dependencies (or a third-party supply chain)?* - *Potential new threats, vulnerabilities or exploitation techniques that could affect the Cloud service are proactively assessed and corrective action is taken?*	
5.2	**Protective monitoring** Providers should monitor for attacks, misuse and malfunction, to help detect successful and unsuccessful attacks against the service as a whole, or the parts of the service that it runs on the Council's behalf. *How can the Council be confident that:* - *The Cloud service generates adequate audit events to provide effective identification of suspicious activity?* - *The collected events are analysed to identify potential compromises or inappropriate use of the Cloud service?* - *The service provider takes prompt and appropriate action to address incidents?*	
5.3	**Incident management** Cloud providers should have pre-planned incident management processes in place, making it more likely that effective and prompt decisions are made when incidents occur, thus minimising the impact to users. *How can the Council be confident that:* - *Incident management processes are in place for the service and are actively deployed in response to security incidents?* - *Pre-defined processes are in place for responding to common types of incidents and attacks?* - *A defined process and contact route exist for customers and external entities to report security incidents and vulnerabilities?*	

	- *The Council will be informed if the service provider detects a security incident that affects the Council's data, in an acceptable, agreed timescale?*	
5.4	**Configuration and change management** Cloud service providers should know what components their service consists of (together with their configurations and dependencies), enabling them to identify and manage changes which could affect the security of the service and fully mitigate vulnerabilities that they are aware of. *How can the Council be confident that:* - *The status, location and configuration of service components (hardware and software) are tracked throughout their lifetime?* - *Changes to the service are assessed for potential security impact, then managed and tracked through to completion?* - *Unauthorised changes to the deployed service components and their configuration will be detected and prevented?* - *The cloud provider will give appropriate notice before making changes that affect how the Council uses the service or its ability to use the service?*	
6	**Personnel security** Customers need to have confidence in the trustworthiness of Cloud service provider's personnel, and the technical measures in place to audit and constrain their actions.	
6.1	**People and security culture** Cloud service providers should ensure that personnel undergo security screening and regular security training, appropriate to their role and privileges. Service providers need to make clear how they screen and manage personnel within any privileged roles. *How can the Council be confident that:* - *The minimum number of people will have access to its data, or could affect its use of the service?*	

	- *The provider has implemented a positive security culture across their organisation?* - *The level of security screening conducted on staff or contractors that have access to Council data or have the ability to affect the service to the Council, is appropriate?*	
6.2	**Technical controls for service administration** Personnel security should combine background checks and procedural controls with technical measures designed to detect and minimise the impact of a malicious insider. *How can the Council be confident that:* - *Administrators accessing Council data, or making changes that affect its use of the service, will be reliably logged and monitored?* - *The Council will be alerted if the provider's personnel perform an action on the cloud service that could (accidentally or otherwise) expose them to Council data?* *What technical controls does the service provider employ to reduce the likelihood of accidental or malicious compromise by personnel carrying out the service?* *Controls should include:* - *Administrators and privileged users given only minimal administrative capabilities temporarily, in response to a specific issue (additional privileges should be requested when necessary)* - *Requests for additional privileges to be linked either to a customer support ticket, or an internal change request* - *Access to systems or interfaces that could provide access to customer data being granted only if the customer has given explicit temporary permission for that access (this applies on a case-by-case basis)*	
7	**Secure development** Cloud Services should be designed, developed and deployed in such a way as to minimise and mitigate threats to their security. If this is not the case, services may be vulnerable to security issues which could compromise customers' data, cause loss of service or enable other malicious activity.	

	How can the Council be confident that: - *The provider utilises a software development lifecycle in line with NCSC's secure software development and deployment guidance, at a standard appropriate for the sensitivity of the Council's data?* - *The Service provider utilises a culture of secure development, including secure development training, code review of all deployed changes, and curation of well-understood libraries for solving security-critical problems?* - *The integration and deployment pipeline used to deliver cloud services is automated to enforce security, consistency, and a detailed audit trail?* - *The production environment is clearly separated from testing and/or development environments?* - *The supply chain of internal and third-party software libraries is managed, ensuring that only external software which is in support is used?* - *External software's security advisories are monitored and security fixes are installed promptly?* - *Configuration and secrets management processes are in place to ensure the integrity of the cloud service throughout development, testing and deployment?* - *Services are kept up to date, in response to new and evolving threats?*	
8	**Supply chain security** Third party supply chains should support all of the security principles which a 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. *During the provision of the Cloud Service:* - *How will the Council's data be shared with, or made accessible to third party suppliers and their supply chains?* - *Which Council data (and metadata derived from that data) will be shared with or made accessible to third party suppliers and their supply chains?* - *How will the Cloud service provider's procurement processes place security requirements on third party suppliers and delivery partners?* - *How will security risks from third party suppliers and delivery partners be managed?* - *How will the management of the conformance of the Cloud service provider's suppliers with security requirements be achieved?*	

9	**Secure user management** Cloud providers should make tools available to securely manage the use of their service, preventing unauthorised access and alteration of customers' resources, applications and data. *How can the Council be confident that:* - *There is a single, well-defined user account model?* - *The Council understands the mechanisms used to authorise access to its data and services, including accesses to management interfaces?* - *The Council is aware of all of the mechanisms by which the service provider would accept management or support requests from Council staff (telephone, web portal, email etc.)* - *Granular access control can be applied, according to the 'principle of least privilege', enabling both 'standard' and 'administrative' user accounts?* - *Other customers cannot access, modify or otherwise affect the Council's service configuration?*	
10	**Identity and authentication** Access to service interfaces should be limited to authenticated and authorised individuals. Services and data should only be accessible to an authenticated and authorised identity, which may be either a user or a service identity. To apply effective access control, customers must have confidence in the authentication method used to determine the identity performing the access. Weak authentication to these interfaces may enable unauthorised access to systems, resulting in the theft or modification of data, changes to the service, or a denial of service. Importantly, authentication should occur over secure channels. *How can the Council be confident that:* - *It understands how access to external interfaces is authenticated?* - *The cloud provider has a modern password policy and requires multi-factor authentication (MFA) for user access?* - *The cloud provider performs equally robust authentication of service identities as it does for users?* - *Authentication of users will integrate with Council processes for managing joiners, movers, and leavers?* - *Processes are available for managing the lifecycle of service credentials?*	
11	**External interface protection**	

	All external or less trusted interfaces to the service should be identified and defended. Defensive measures may include application programming interfaces (APIs), web consoles, command line interfaces (CLIs), or direct connect services. Also, the cloud provider's administration interfaces, the interfaces customers use to access the service, and any interfaces to customers' services built on top of the cloud service. If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant. Different models can be used to connect to cloud services which expose customers' enterprise systems to varying levels of risk. *How can the Council be confident that:* - *It understands what physical and logical interfaces to Council information exist, and how access to Council data is controlled?* - *The Cloud service identifies and authenticates users to an appropriate level over those interfaces?*	
12	**Secure service administration** Cloud providers should recognise the high value of administration systems. The design, implementation, and management of the administration systems utilised by cloud providers should follow enterprise good practice, whilst recognising their high value to attackers. Systems used by providers for the administration of their cloud services will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. *How can the Council be confident that the Cloud Service provider:* - *Builds and maintains trust in the devices it uses to administer the service, with regular and thorough security assessments?* - *Protects its administration interfaces?* - *Risk-manages its administration using tiers?* - *Uses privilege access management, including 'just in time' and 'just enough' administration?* - *Uses administration interfaces that produce detailed audit information, which is checked regularly for anomalous or unexpected behaviour?*	

13	**Audit information and alerting for customers** Cloud Providers should supply logs needed to monitor access to a Cloud service and the data held within it. Customers should be able to identify security incidents and have the information necessary to determine how and when they occurred.	
13.1	**Audit information** Customers should be provided with the audit data needed to investigate incidents related to their use of the Cloud service and the data held within it. The type of audit information available to customers will have a direct impact on their ability to respond to inappropriate or malicious activity within reasonable timescales. *How can the Council be confident that:* - *It is aware of the audit information that will be provided, how and when it will be made available, the format of the data, and the retention period associated with it?* - *The audit information available will be sufficient for investigating misuse or incidents?* - *The provider will supply relevant audit information for actions taken by its personnel that affect the service (or the data held within it)?* - *Audit information cannot be deleted by the Council or the Cloud provider during a defined retention period?*	
13.2	**Security alerts** Customers should be alerted when the Cloud provider detects attacks against their data or their use of the provider's services. The Cloud provider should be the customers' first line of defence for identifying and preventing common attacks. *How can the Council be confident that:* - *The provider will alert the Council when it identifies attacks against, or vulnerabilities in, the Council's use of their services?* - *The provider will alert the Council when it detects attempted or successful compromise of Council's data held in their services?* - *The provider will send their alerts promptly to a recipient of the Council's choosing, through an automated means?*	

14	**Secure use of the service** Cloud Service providers should make it easy for their customers to meet their responsibility to adequately protect their data.	
14.1	**Security by design and default** Cloud Service providers should make it easy for their customers to use their services in a way that is defended against common attacks. *How can the Council be confident that:* - *It knows which goals from the Principles 1-13 are met by the service's default configuration?* - *It knows what it needs to do to the service's configuration to meet the remaining goals?* - *Data and services are not accessible to unauthenticated users, by default?* - *The provider takes responsibility for improving their service's default configuration, to respond to new threats (this may include altering the configuration of existing customers, as well as changing the starting point for new customers)?*	
14.2	**Help customers meet their security responsibilities** Cloud Service providers should make it easy for their customers to be confident that they are using the cloud securely. It should be easy for customers to see what services they have in the cloud, and how they have been configured. *How can the Council be confident that:* - *All service configurations can be set and audited using infrastructure as code, or via an API?* - *There is a single place where the Council can see all of its deployed resources across all services and regions offered by the cloud platform?* - *All service configurations are visible and intuitive to humans, so that they can easily audit what services they are using, where their data is, and how those services are configured?*	