Cloud Security Standards and Guidelines

V2

Version:	**2**
Dated:	**16 Sept 2019**
Document Owner:	**Head of IT Security and Compliance**

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
0.1	May 2018	Ali Mitchell	New document
1	May 2018	Ali Mitchell	Approved version
1.1	July 2019	Ali Mitchell	Removed and added new links to policy documents in paragraph 4 Changed roles in paragraph 5 (removed steward) Added in paragraph 5.3 (about DPIAs) Amended paragraphs 6.2.3, 6.2.3, 6.15.2
2	Sept 2019	Ali Mitchell	Ready for IGSSG – 19 Sept 19

Review Distribution

Name	Title
Rhiannon Platt	Information Governance Manager and Data Protection Officer
Mike Maling	Operations and Security Manager
Duncan Hepple	Senior Cloud and Services Engineer
Matt Harvey	Lead Cloud Services Engineer
Ian Tilsed	Assistant Director Strategy and Architecture

Approval

Version	Position	Signature	Date
1	Members of the IGSSG		May 2018
2	Members of the IGSSG		

Contents

1. Introduction

1.1 It is essential that the University has a clear picture of the risks involved when adopting new information systems, especially those that are hosted in the Cloud. When systems are deployed on the University's estate, we include mechanisms to reduce the chances of cyber security problems occurring and implement measures which minimise the impact of a cyber-attack. The University is committed to safeguarding its information and data, including individual's personal data and it is therefore necessary that the same level of security controls are applied to new and existing information systems in the Cloud.

1.2 These standards are mostly based upon the 14 Cloud Security Principles as outlined by the National Cyber Security Centre.

2. Purpose

2.1 These standards outline the University's expectations for security control implementations within a Cloud service, and aid in determining whether a specific Cloud service is secure enough to handle the University's information destined for it.

3. Scope

3.1 These standards apply to all Cloud-based applications and services used for the processing, storage and transportation of University information that if disclosed publicly without authorisation, could result in financial, commercial or reputational damage and/or legal proceedings.

3.2 These standards apply to any provider of any such system.

3.3 These standards apply to any University member responsible for the selection of any such system on behalf of the University.

4. Related Policies and Documents

- Cloud Security Standards Supplier Assessment
- Cloud Security Standards Supplier Survey
- Overarching Information Governance and Security Policy
- Data Breach Policy
- Information Security Controls Policy
- Privacy and Personal Data Protection Policy

5. Preparation and Asessment of Suitability

5.1 When considering any new information system, identify the roles of Senior Information Risk Owner (SIRO), System Owner (SO), and Information Asset Owner (IAO), as outlined in University's Data Protection Policy. Establishing these roles from the outset is key to ensure that all risks to information are considered during the selection process.

5.2 SOs and IAOs should work to establish the information that will be processed, stored or transported by the cloud service, and understand the legal and regulatory implications. For example, if personal data is to be stored or processed then the chosen solution must be fully compliant with University's Data Protection Policy.

5.3 As a minimum a Data Protection Impact Assessment (DPIA) should be conducted in order to understand the types of data being processed or stored by the cloud solution / platform. No system should go live until the DPIA has been reviewed and approved by the Information Governance team, IT Security and Compliance team and the relevant IAO.

5.4 A full assessment of each Cloud solution provider being considered, should be carried out with the support of the IT Security and Compliance team. The assessment will be carried out against the standards within this document in order to give a complete picture of the risks to information the University is likely to face by selecting a specific solution.

5.5 If the outcome of such an assessment determines that the security control implementations of a provider do not meet the minimum required standard, or fail to meet the objectives of the University's Information Security Policy, and Data Protection Policy, the provider should be considered unsuitable. Again, a system should not go live without the review and approval of a DPIA.

6. Principles and Implemenatations

6.1 Data in Transit Protection

6.1.1 User data transiting networks should be adequately protected against tampering and eavesdropping. This should be achieved through a combination of network protection and encryption.

6.1.2 Information system owners should be sufficiently confident that "data in transit" is protected between end users and the service, internally within the service, and between the service and other services.

6.1.3 The University prefers that data in transit be protect by TLS (Version 1.2 or above), configured in line with best practise (e.g. as outlined by companies such as Qualys, Google or Mozilla). IPsec or TLS VPN gateways may also be considered. Legacy TLS/SSL will not be accepted for new services.

6.2 Physical Location

6.2.1 In order to understand the legal circumstances under which data could be accessed without the University's consent you must identify the locations at which it is stored, processed and managed.

6.2.2 Information system owners should understand in which countries data will be stored, processed and managed and how this relates to compliance with relevant legislation e.g. General Data Protection Regulation. Please note that any data centres being used should be based in the EU.

6.2.3 If any data contains personal data (as defined by data protection legislation), then it must only be transferred to a location in accordance with the University's Data Protection Policy and relevant legal frameworks.

6.3 Data Centre Security

6.3.1 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.

6.3.2 SOs should be confident that the physical security measures implemented by the provider are in line with the University's expectations.

6.3.3 The University expects that data centres used by Cloud providers have had their data centre protections certified against a recognised and appropriate standard that covers physical security.

6.4 Data at Rest Protection

6.4.1 To ensure data is not available to unauthorised parties with physical access to infrastructure, University data held within the service should be protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.

6.4.2 SOs should be sufficiently confident that storage media containing University data are protected from unauthorised access and where personal data is contained, should be encrypted.

6.4.3 The University expects that data at rest will be protected by physical access controls that have been certified against a recognised and appropriate standard (as covered by 6.3.) or that protection is achieved through encryption of all physical media.

6.5 Data Sanitisation

6.5.1 The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data. Inadequate sanitisation of data could result in data being retained by the service provider indefinitely, data being accessible to other users of the service as resources are reused, or data being lost or disclosed on discarded, lost or stolen media.

6.5.2 SOs should be sufficiently confident that data is erased when resources are moved or re-provisioned, when they leave the service or when a request for it to be erased is made and that storage media which has held data is sanitised or securely destroyed at the end of its life.

6.5.3 The University requires assurances around how storage is reallocated, especially if encryption is not employed as part of protecting data at rest.

6.6 Equipment Disposal

6.6.1 Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.

6.6.2 SOs should be sufficiently confident that all equipment potentially containing University data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled), that any components containing sensitive data are sanitised, removed or destroyed as appropriate, and that any accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.

6.6.3 The University expects that either a recognised standard for equipment disposal is followed or that a third-party destruction service assessed against a recognised standard is used.

6.7 Physical Resilience and Availability

6.7.1 Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on the University.

6.7.2 SOs should be sufficiently confident that the availability commitments of the service, including their ability to recover from outages, meets your business needs.

6.7.3 The University requires that availability requirements are met via contractual commitments from the provider. A review of historical records of availability may provide additional assurance.

6.8 Separation Between Users

6.8.1 A malicious or compromised user of a service (i.e. another customer of the provider) should not be able to affect the service or data of the University.

6.8.2 SOs should be sufficiently confident that the service provides sufficient separation from other users of the service, and be confident that the management of the service is kept separate from other users.

6.8.3 The University expects providers to utilise a range of technical controls to achieve sufficient user separation, for example a combination of virtualisation technologies and other software controls. Additional assurances may be required in certain circumstances.

6.9 Governance Framework

6.9.1 The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Having an effective governance framework will ensure that procedure, personnel, physical and technical controls continue to work through the lifetime of a service.

6.9.2 SOs should be sufficiently confident that the service has a governance framework and processes which are appropriate for the service. 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 relevant to the service.
- Security and information security are part of the service provider’s financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk.

- Processes to identify and ensure compliance with applicable legal and regulatory requirements.

6.9.3 The University prefers providers that conform to a recognised standard such as ISO/IEC 27001, however the scope of any certification should be validated. Providers only able to offer assertions that the objectives outlined in 6.9.2. are met should be further evaluated to determine whether any associated risks are acceptable.

6.10 Configuration and Change Management

6.10.1 The University should have an accurate picture of the assets which make up the service, along with their configurations and dependencies. Changes which could affect the security of the service should be identified and managed. Unauthorised changes should be detected. Where change is not effectively managed, security vulnerabilities may be unwittingly introduced to a service. And even where there is awareness of the vulnerability, it may not be fully mitigated.

6.10.2 SOs should have confidence that the status, location and configuration of service components (both 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.

6.10.3 The University prefers providers that conform to a recognised standard such as ISO/IEC 27001, however the scope of any certification should be validated to verify that configuration and change management were covered. Providers only able to offer assertions that the objectives outlined in 6.10.2. are met should be further evaluated to determine whether any associated risks are acceptable.

6.11 Vulnerability Management

6.11.1 Service providers should have management processes in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools.

6.11.2 SOs have confidence that potential new threats, vulnerabilities or exploitation techniques which could affect your service are assessed and corrective action is taken within an acceptable timeframe.

6.11.3 The University expects that providers will support patching or vulnerability management within the timescales set out below:

- If there is evidence to suggest that a vulnerability is being exploited in the wild, mitigations should be put in place **immediately.**
- If there is no evidence that a vulnerability is being actively exploited, the following timescales are considered as the minimum[1]:
    - **Critical –** patches should be deployed within hours
    - **Important –** patches should be deployed within 14 days of a patch becoming available

[1] 'Critical', 'Important', and 'Other' are aligned to common vulnerability scoring systems such as NVD (which is in turn aligned with CVSS), and Microsoft's Security Bulleting Severity Rating System.

- **Other –** patches should be deployed within 8 weeks of a patch becoming available

6.12 Protective Monitoring

6.12.1 A service which does not effectively monitor for attack, misuse and malfunction will be unlikely to detect attacks (both successful and unsuccessful). As a result, it will be unable to quickly respond to potential compromises of University environments and data.

6.12.2 SOs should have confidence that the service generates adequate audit events to support effective identification of suspicious activity, and that these events are analysed to identify potential compromises or inappropriate use of the service and that the service provider takes prompt and appropriate action to address incidents.

6.12.3 The University prefers providers that conform to a recognised standard such as ISO/IEC 27001, however the scope of any certification should be validated to verify that protective monitoring controls were covered. Providers only able to offer assertions that the objectives outlined in 6.12.2. are met should be further evaluated to determine whether any associated risks are acceptable.

6.12.4 If it is determined to be the responsibility of the University to monitor use of the service, consideration should be given to the University's access to, and capability to effectively analyse, accounting and audit information in order to satisfy the objectives outlined in 6.12.2.

6.13 Incident Management

6.13.1 Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur, potentially exacerbating the overall impact on users. These processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service.

6.13.2 SOs should have confidence that incident management processes are in place for the service and are actively deployed in response to security incidents. They should also be confident that a defined process and contact routes exist in order that the University may report security incidents, and that the provider will make the University aware of relevant security incidents within an acceptable timescale and format.

6.13.3 The University prefers providers that conform to a recognised standard such as ISO/IEC 27001, however the scope of any certification should be validated to verify that incident management controls were covered. Providers only able to offer assertions that the objectives outlined in 6.13.2. are met should be further evaluated to determine whether any associated risks are acceptable.

6.14 Personnel Security

6.14.1 Where service provider personnel have access to University data, a high degree of trustworthiness is required.

6.14.2 SOs should be sufficiently confident that the level of security screening conducted on service provider staff with access to your information, or with ability to affect the service is

appropriate. They should also be confident that the minimum number of people necessary have access to University information or could affect the service.

6.14.3 The University prefers that personnel screening is in place which includes or exceeds the requirements of BS7858:2012.

6.15 Secure Development

6.15.1 Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise University data, cause loss of service or enable other malicious activity.

6.15.2 Information system owners should be sufficiently confident that new and evolving threats are reviewed and the service improved in line with them, and that development is carried out in line with industry good practice regarding secure design, coding, testing and deployment. They should also be confident that configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.

6.15.2 The University expects that providers will adhere to University supplied technical security controls which are supplied by the IT Security and Compliance team and where required will substantiate this by way of independent validation.

6.16 Supply Chain Security

6.16.1 The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

6.16.2 SOs should be sufficiently confident that third party products and services relied upon by the service do not undermine the security of the service by failing to implement any of these principles.

6.16.3 The University expects that the security objectives within these standards are transited throughout the provider's supply chain. Due to the complexity of assessing controls implemented throughout the supply chain, it is preferred that these aspects are covered through the application of an appropriate standard. Any certification should be checked to ensure that the scope of assessment covered the supply chain aspects required.

6.17 Authentication of Users to Management Interfaces and Support Channels

6.17.1 Service providers need to ensure that all management requests which could have a security impact are performed over secure and authenticated channels. If users are not strongly authenticated then an imposter may be able to successfully perform privileged actions, undermining the security of the service or data.

6.17.2 SOs should be aware of all of the mechanisms by which the service provider would accept management or support requests from the University (telephone, web portal etc.), and that only authorised individuals from the University can use those mechanisms to affect the service.

6.17.3 The University expects that strong authentication for these channels is in place, and that adequate safeguards are in place to prevent circumvention of any controls (e.g. social engineering attacks).

6.18 Separation and Access Control within Management Interfaces

6.18.1 Many cloud services are managed via web applications or APIs ('application programming interface'). These interfaces are a key part of the service's security. If users are not adequately separated within management interfaces, one user may be able to affect the service, or modify the data of another.

6.18.2 SOs must understand how management interfaces are protected and what functionality is exposed, and should be sufficiently confident that other users cannot access, modify or otherwise affect management of the service. Any risks associated to privileged access should be appropriately managed.

6.18.3 The University expects that management interfaces are designed in a way that can be appropriately secured and maintained in line with other University Information Security Policies.

6.19 Identity and Authentication

6.19.1 All access to service interfaces should be constrained to authenticated and authorised individuals.

6.19.2 SOs should be sufficiently confident that identity and authentication controls ensure users are authorised to access specific interfaces.

6.19.3 The University requires that services can be integrated with standard University identity management and authentication systems in accordance with other University Information Security Policies. This may be combined with other approaches such as limited access over a dedicated link.

6.20 External Interface Protection

6.20.1 All external or less trusted interfaces of the service should be identified and appropriately defended.

6.20.2 SOs should understand what physical and logical interfaces University information is available from, and how access to the data is controlled. They should be confident that the service identifies and authenticates users to an appropriate level over those interfaces.

6.20.3 The University expects that any interfaces exposed publicly (e.g. over the internet), have been designed to be robust to attack, and that the provider has a regime of continuous testing in place to ensure those interfaces remain secure.

6.21 Secure Service Administration

6.21.1 Systems used for administration of a cloud service 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.

6.21.2 SOs should understand the service administration model in use, and ensure that any risks are acceptable.

6.21.3 The University expects that service providers are able to provide detailed information on the system administration model[2] used to administer the service. Any associated risks will be evaluated in accordance with other University Information Security Policies.

6.22 Audit Information for Users

6.22.1 The University require audit records to monitor access to the service and the data held within it. The type of audit information available will have a direct impact on our ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

6.22.2 SOs should be aware of the audit information provided, how and when it will be made available, the format of the data, and the retention period associated with it, and be sufficiently confident that the audit information available will meet our needs for investigating misuse or incidents.

6.22.3 The University must be able to satisfy a number of legal and regulatory requirements. It is expected that audit information made available will enable the University to meet these requirements (if you are unsure of the requirements relating to the service being considered, please contact the University Legal Team and/or the Information Governance Manager.

6.23 Secure Use of the Service

6.23.1 The security of the service and the data held within it can be undermined if University staff fail to use the service in an appropriate way.

6.23.2 SOs should understand any service configuration options available and the security implications of any choices made, as well as ensure that staff are appropriately trained in using and managing the service in line with other University Information Security Policies.

6.23.3 The University expects that service providers are able to support the University in using the service securely, but recognises that University staff must be made aware of their responsibilities in this regard, and that their use of the service does not undermine the objectives within these standards or associated University policies.

7. Help and Advice

7.1 For any queries relating to this document email the IT Security and Compliance team itsecurityandcompliance@exeter.ac.uk

[2] Some common approaches are detailed by the NCSC here: https://www.ncsc.gov.uk/guidance/systems-administration-architectures