Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.5	**Information Security Policies**								
A.5.1	Management direction for information security	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.							
A.5.1.1	The policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	yes	yes	yes	yes	yes	yes	legal risk assessment business requirement best practice
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	yes	yes	yes	yes	yes	yes	legal risk assessment business requirement best practice
A.6	**Organization of information security**								
A.6.1	Internal organization	Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.							

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.6.1.1	Information Security Roles and Responsibilities	All information security responsibilities shall be defined and allocated.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.6.2	Mobile devices and teleworking	Objective: To ensure the security of teleworking and use of mobile devices.							

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.7	**Human resource security**								
A.7.1	Prior to employment	Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.							
A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	yes	yes	yes	yes	yes	yes	legal risk assessment business requirement best practice
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	yes	yes	yes	yes	yes	yes	legal business requirement best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.7.2	During employment	Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.							
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice risk assessment
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.7.3	Termination and change of employment	Objective: To protect the organization's interests as part of the process of changing or terminating employment.							
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.8	**Asset management**								
A.8.1	Responsibility for assets	Objective: To identify organizational assets and define appropriate protection responsibilities.							
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.8.2	Information classification	Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.							
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment
A.8.3	Media handling	Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.							
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	yes	yes	yes	yes	yes	yes	business requirement best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.9	**Access control**								
A.9.1	Business requirements of access control	Objective: To limit access to information and information processing facilities.							
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.9.2	User access management Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.								
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	yes	yes	yes	yes	yes	yes	risk assessment legal best practice business requirement
A.9.3	User responsibilities	Objective: To make users accountable for safeguarding their authentication information.							
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.9.4	System and application access control	Objective: To prevent unauthorized access to systems and applications.							
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.10	**Cryptography**								
A.10.1	Cryptographic controls	Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.							
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.11	**Physical and environmental security**								
A.11.1	Secure areas	Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.							
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.11.2	Equipment	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.							
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	yes	yes	yes	yes	yes	yes	best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	yes	yes	yes	yes	yes	yes	risk assessment best practice
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.12	**Operations security**								
A.12.1	Operational procedures and responsibilities	Objective: To ensure correct and secure operations of information processing facilities.							
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.12.2	Protection from malware	Objective: To ensure that information and information processing facilities are protected against malware.							
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.12.3	Backup	Objective: To protect against loss of data.							
A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.12.4	Logging and monitoring	Objective: To record events and generate evidence.							

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.12.5	Control of operational software	Objective: To ensure the integrity of operational systems.							
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.12.6	Technical vulnerability management	Objective: To prevent exploitation of technical vulnerabilities.							
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.12.7	Information systems audit considerations	Objective: To minimise the impact of audit activities on operational systems.							
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.13	**Communications security**								

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.13.1	Network security management	Objective: To ensure the protection of information in networks and its supporting information processing facilities.							
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.13.2	Information transfer	Objective: To maintain the security of information transferred within an organization and with any external entity.							
A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.14	**System acquisition, development and maintenance**								
A.14.1	Security requirements of information systems	Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.							
A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	yes	yes	yes	yes	yes	yes	best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.14.2	Security in development and support processes	Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.							
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	no	n/a	n/a	n/a	n/a	n/a	system or software development is not outsourced risk assessment
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	yes	yes	yes	yes	yes	yes	best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.14.3	Test data	Objective: To ensure the protection of data used for testing.							
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.15	**Supplier relationships**								
A.15.1	Information security in supplier relationships	To ensure protection of the organization's assets that is accessible by suppliers.							
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	yes	yes	yes	yes	yes	yes	legal best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.15.2	Supplier service delivery management	Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.							
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	yes	yes	yes	yes	yes	yes	best practice risk assessment
A.16	**Information security incident management**								
A.16.1	Management of information security incidents and improvements	Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.							

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.17	**Information security aspects of business continuity management**								
A.17.1	Information security continuity	Objective: Information security continuity shall be embedded in the organization's business continuity management systems.							
A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.17.2	Redundancies	Objective: To ensure availability of information processing facilities.							
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	yes	yes	yes	yes	yes	yes	risk assessment best practice business requirement
A.18	**Compliance**								
A.18.1	Compliance with legal and contractual requirements	Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.							
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	yes	yes	yes	yes	yes	yes	legal best practice risk assessment
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	yes	yes	yes	yes	yes	yes	legal best practice business requirement risk assessment
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	yes	yes	yes	yes	yes	yes	legal risk assessment best practice business requirement
A.18.2	Information security reviews	Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.							
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	yes	yes	yes	yes	yes	yes	best practice business requirement risk assessment
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	yes	yes	yes	yes	yes	yes	best practice risk assessment

Databricks ISO 27001 / 27018 / 27017 Statement of Applicability.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27001:2013		ISO 27018:2019		ISO 27017: 2015		
Section	Section Title	Section Objective	Included	Implemented	Included	Implemented	Included	Implemented	Justification for inclusion
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	yes	yes	yes	yes	yes	yes	best practice risk assessment

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion
A.2	**Consent and Choice**				
A.2.1	Obligation to co-operate regarding PII principals' rights	The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.3	**Purpose Legitimacy and Specification**				
A.3.1	Public cloud PII processor's purpose	PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.3.2	Public cloud PII processor's commercial use	PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.5	**Data Minimization**				
A.5.1	Secure erasure of temporary files	Temporary files and documents should be erased or destroyed within a specified, documented period.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.6	**Use, Retention and Disclosure Limitation**				

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion
A.6.1	PII Disclosure Notification	The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.6.2	Recording of PII disclosures	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.8	**Openness, Transparency and Notice**				
A.8.1	Disclosure of sub-contracted PII processing	The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.10	**Accountability**				
A.10.1	Notification of a data breach involving PII	The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.10.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion
A.10.3	PII return, transfer and disposal	The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11	**Information Security**				
A.11.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.3	Control and logging of data restoration	There should be a procedure for, and a log of, data restoration efforts.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.4	Protecting data on storage media leaving the premises	PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.5	Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion
A.11.6	Encryption of PII transmitted over public data-transmission networks	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.8	Unique use of user IDs	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.10	User ID management	De-activated or expired user IDs should not be granted to other individuals.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.11	Contract measures	Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27018 Appendix A Statement of Applicability. Public cloud PII processor extended control set for PII protection.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27018:2019 Appendix A		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion
A.11.12	Sub-contracted PII processing	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.11.13	Access to data on pre-used data storage space	The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.12	**Privacy Compliance**				
A.12.1	Geographical location of PII	The public cloud PII processor should specify and document the countries in which PII might possibly be stored.	Yes	Yes	Public cloud PII processor extended control set for PII protection
A.12.2	Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	Yes	Yes	Public cloud PII processor extended control set for PII protection

Databricks ISO 27017 Appendix B Statement of Applicability. Cloud service providers and customers extended control set for provision and user of cloud services.

ISMS
Last updated: 6/23/2021 version 5
Company Confidential. If printed, this is not the authoritative version.

			ISO 27017 : 2015 Appendix B		
Section	Section Title	Section Objective	Included	Implemented	Justification for inclusion or exclusion
CLD.6.3	**Relationship between cloud service customer and cloud service provider**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.8.1	**Responsibility for assets**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.8.1.5	Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.9.5	**Access control of cloud service customer data in shared virtual environment**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services

CLD.9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.12.1	**Operational procedures and responsibilities**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.	Yes	Yes	Cloud service providers and customers extended control set for provision and user of cloud services
CLD.12.4	**Logging and monitoring**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.12.1.5	Monitoring of Cloud Services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	Yes	Yes	Cloud service providers and customers extended control
CLD.13.1	**Network security management**	**To ensure that the information security is implemented and operated in accordance with the organizational security policies and standards.**			
CLD.13.1.4	Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.	Yes	Yes	Cloud service providers and customers extended control