NORTON ROSE FULBRIGHT

Supplier information security standard

October 2023

Information Security Policy and Management

1.1 Supplier must establish and maintain an information security program that includes appropriate information security policies and procedures for the size of operations and the sensitivity of information handled on behalf of Norton Rose Fulbright.

1.2 The information security program of Supplier must include appropriate organizational and technical measures aligned with industry standards of best practice to protect information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and nature of the information to be protected.

1.3 Supplier's information security policies must be periodically reviewed, updated and approved by Supplier management. Supplier must communicate in writing information security requirements to all Supplier personnel contributing to Services provided to Norton Rose Fulbright.

Points of contact

2.1 In situations that require Supplier to contact Norton Rose Fulbright in regards to information security, as detailed in this Standard, Norton Rose Fulbright's IT Global Service Desk Contact details are: by phone: +44 (0) 207 444 5555 and by email: 5555@nortonrosefulbright.com.

2.2 Supplier must designate an individual who will serve as Norton Rose Fulbright's ongoing single point of contact for purposes of addressing issues with respect to the use and security of Norton Rose Fulbright Confidential Information.

Third-Party Relationships

3.1 Supplier must notify Norton Rose Fulbright before Supplier transfers, subcontracts or outsources any or all of its obligations to provide the Services to a third party, and in any such notice shall include the name and address of the third-party vendor.

3.2 Supplier must require of all its third-party vendors that host, process or access Norton Rose Fulbright Confidential Information to implement security measures aligned with this Standard. Supplier must establish procedures to review and verify that all third-party vendors that have access to Norton Rose Fulbright Confidential Information are managed to limit risk exposure to Norton Rose Fulbright. Third-party vendors must be reviewed by Supplier periodically and assessed for information security risks.

3.3 Without prejudice to any other liability Supplier may have or any other claim Norton Rose Fulbright may have, Supplier shall be fully responsible for all and any works, services, materials, drawings, documents and acts, breaches, omissions, defaults and/or negligence or failure of any of its third-party vendors as if it was the act, breach, omission, default, neglect or failure of Supplier.

3.4 If Supplier proposes using a cloud environment to process or store Norton Rose Fulbright Confidential Information, Supplier must only use a privately hosted or dedicated cloud environment that encrypts information while at rest, and stores it in accordance with the terms of this Agreement, including without limitation section 5.2 of this Standard.

Retention, Return and Destruction of Information

4.1 Supplier must retain Norton Rose Fulbright Confidential Information only for as long as specified by Norton Rose Fulbright or as necessary for the provision of the Services, except to the extent that longer retention is required by applicable law or regulations.

4.2 Upon request from Norton Rose Fulbright, Supplier will:

i. Destroy Norton Rose Fulbright Confidential Information under its control.

ii. Provide confirmation that Norton Rose Fulbright Confidential Information has been irretrievably destroyed.

Exchange, Transfer and Storage of Information

5.1 Supplier must protect all Norton Rose Fulbright Confidential information in transit and in storage, including:

i. Encrypt all Norton Rose Fulbright Confidential Information that resides on systems, servers, storage media, and backup media controlled by Supplier, including Norton Rose Fulbright Confidential Information that resides on the systems and servers of any third party with which Supplier has subcontracted to process or store electronic data;

ii. Use encryption when transferring Norton Rose Fulbright Confidential Information, and in communications between Supplier and Norton Rose Fulbright or between Supplier and any third party with which Supplier has subcontracted to process or store electronic data. Supplier's systems used for email or web services must be configured to automatically encrypt communications between Supplier and Norton Rose Fulbright with Transport Layer Security (TLS);

iii. In the event that Norton Rose Fulbright Confidential Information could be transferred to removable media or a mobile electronic device such as a smartphone, tablet or laptop, implement, monitor, and maintain encryption and information leakage prevention tools.

5.2 Supplier must:

i. Maintain physical or logical separation between Norton Rose Fulbright Confidential Information and information belonging to other parties, such as other clients of Supplier, to prevent malicious or compromised third parties from affecting the Services;

ii. Only host, store, access or process Norton Rose Fulbright Confidential Information in or from Agreed Locations;

iii. Not, without obtaining the prior written consent of Norton Rose Fulbright, change the location where Norton Rose Fulbright Confidential Information is hosted, stored, accessed or processed, or otherwise disclose or transfer Norton Rose Fulbright Confidential Information to any person or entity located outside of an Agreed Location.

Logical Access Control Management

6.1 Supplier must have logical access controls designed to manage access to information and system functionality on a least privilege and need-to-know basis, including:

i. Identify and document administrative user accounts and types, and their level of access. Revoke accounts when they are no longer required. Additionally, promptly change passwords if it is likely that they have become known by someone else or otherwise compromised;

ii. Authenticate access to information, maintain user and privileged accounts in conformance with industry and commercially reasonable standards, and regularly review access privileges to information and revoke access when it is no longer required;

iii. Secure privileged access using strong authentication methods;

iv. Protect all stored user passwords, passphrases, and PINs with one-way encryption solutions and secure privileged access using strong authentication methods;

v. Require a two-factor authentication for remote access to information assets controlled by Supplier.

Human resource security

7.1 Screening of personnel

Background checks must be performed on all Supplier personnel who have access to Norton Rose Fulbright Confidential Information. The scope must include, at a minimum, identity check, verification of education qualifications or other skills claimed, criminal record check, financial checks, and verification of relevant licenses and certifications, where permitted by law.

7.2 Training of personnel

Supplier must ensure that all Supplier personnel who have access to Norton Rose Fulbright Confidential Information receive information security awareness training and regular updates in Supplier's policies and procedures, as relevant for their job function.

Physical and environmental security

8.1 Supplier must ensure that appropriate safeguards are in place to achieve the following:

i. Physically protect any facility where Norton Rose Fulbright Confidential Information is accessed, stored, processed, or destroyed using industry standard security barriers and entry controls such as access cards, walls and manned reception desks; protect equipment used by Supplier for the storage, processing or destruction of Norton Rose Fulbright Confidential Information against power failures and other disruptions caused by failures in supporting utilities;

ii. Log access to the facilities and securely maintain such logs; authenticate, escort and supervise visitors and guests at all times while they are on premise.

System Administration and Network Security

Supplier must have operational procedures and controls designed to ensure that technology and information systems are configured and maintained according to prescribed internal policies and standards and consistent with applicable standards of best practice. In particular, Supplier must implement and maintain the security controls listed in this section, as applicable:

9.1 Protection against malware and malicious access

i. Install protection against malware on systems controlled by Supplier and configure it to automatically search for and download updates (daily, at a minimum) and perform continuous virus scans. Malware and threat detection is to be updated continuously, and software patches provided by vendors must be downloaded and implemented in a timely manner;

ii. Put in place controls to filter and block malicious or inappropriate content and implement advanced persistent threat management capability to protect systems storing or processing information;

9.2 Network security

i. Configure network devices, including routers and switches, according to approved lockdown standards. Govern and monitor changes to network security controls using change management standards;

ii. Implement and maintain firewalls, segmented network zones, intrusion detection systems and intrusion prevention systems designed to protect systems from intrusion or limit the scope or success of any attack or attempt at unauthorized access to information;

iii. Establish port, protocol and IP address restrictions that limit the inbound and outbound network traffic to the minimum required. All inbound traffic must be routed to specific and authorized destinations;

iv. Regularly scan applications, operating systems and technology infrastructure related to the Services for security vulnerabilities and resolve findings in a timely manner;

9.3 System maintenance

i. Adopt and follow patching procedures for applications, operating systems and technology infrastructure to mitigate and protect against new and existing security vulnerabilities and threats in a timely manner;

ii. Adopt and follow procedures to maintain versions of applications, operating systems and technology infrastructure that are supported by their respective manufacturers, and to properly decommission applications, operating systems and technology infrastructure before they reach their manufacturer's end-of-life date;

9.4 Supplier workstation and user device security

i. Implement and maintain controls on workstations and user devices under Supplier's control, including mobile communication devices and portable storage devices, to prevent unauthorized access, leakage, unauthorized alteration or destruction of information;

9.5 Back-ups

i. Create, encrypt, maintain and securely store daily backups of Norton Rose Fulbright Confidential Information stored on systems controlled by Supplier and any applications or configuration information necessary to provide the Services, and regularly test back-up copies of Norton Rose Fulbright Confidential Information;

ii. Implement a procedure for handling back-up copies to prevent the theft or loss of Norton Rose Fulbright Confidential Information, take adequate steps to protect back-up copies while in transit and keep backup copies of Norton Rose Fulbright Confidential Information in a secure and controlled place, in accordance with instructions from Norton Rose Fulbright, if any;

9.6 Services Resilience

i. Implement disaster recovery and business continuity plans describing the procedures which will be applied to ensure the continued performance of the Services should an event diminish or disrupt Supplier's ability to render the Services or maintain the agreed-upon levels of service;

ii. In the event of a disaster or emergency, ensure that it has planned a sufficient recovery capacity internally as well as externally to support its business continuity and recovery plans;

iii. Regularly test (at least once per year) its business continuity plan and disaster recovery plan which will ensure the continued performance of the Services, and implement any corrective measures identified as necessary after the test;

iv. Protect Services that host or process Norton Rose Fulbright Confidential Information against denial of service attacks by implementing denial-of-service mitigation solutions.

Logging and monitoring

10.1 Supplier must

i. Implement logging of activity in the Services and infrastructure, including activity related to access or attempt to access, to support investigations of suspected security incidents or malicious activity;

ii. Assign unique identifiers to all application users within each application;

iii. Maintain application log files that record and timestamp, for all application users: successful and unsuccessful log-on attempts, and actions performed by each user;

iv. Protect logs against unauthorized access or modification, and retain such logs for at least six months; Logs must not be deleted or overwritten in this period unless the data has been first forwarded to a centralized log repository (e.g., SIEM) for retention;

v. Upon request from Norton Rose Fulbright, make available to Norton Rose Fulbright any logs that may help Norton Rose Fulbright monitor access to Norton Rose Fulbright Confidential Information.

Application and Web Development Security

11.1 To the extent applicable, Supplier must:

i. Establish rules for the development of software and systems and apply such rules to developments within Supplier. Information security must be designed and implemented within the development lifecycle of information systems;

ii. Follow recognised industry secure development practices for all software code development, including implementing processes to protect program source code and test data, and to validate the input, internal processing, and output of data in applications;

iii. Perform pre-deployment and ongoing security assessments of any Internet-accessible applications;

iv. Develop any Internet-accessible applications based on secure coding guidelines such as those found in the Open Web Application Security Project (OWASP) Development Guide.

11.2 Norton Rose Fulbright Confidential Information must not be used in development or testing environments of Supplier without the prior consent of Norton Rose Fulbright. If Norton Rose Fulbright Confidential Information must be used for testing purposes, Supplier must ensure that it has in place processes to achieve the following controls:

i. Set up a mechanism deleting any sensitive content (data masking) and making the data anonymous;

ii. Securely delete the data from development or testing environments at the end of testing.

11.3 Other than as set out in the Agreement and to the extent applicable, Supplier without the prior written consent of Norton Rose Fulbright, must not:

i. Use Norton Rose Fulbright Confidential Information to train, calibrate, query, upload or otherwise into, any generative AI Services or associated model including machine learning technology; or

ii. Use any requirement for data or information to be other than for the provision of the Services, including not merging any such data or information with any Supplier general data pool.

Management and notification of security breaches

12.1 Supplier must implement and maintain an information security incident management procedure (covering the loss of availability, integrity or confidentiality of information). Such procedure must include the reporting, diagnosis, treatment according to the level of severity, escalation and communication procedure, documentation and follow-up, as well as debriefing documentation for the incident. Supplier will review its information security incident management procedure periodically.

12.2 Upon discovering a security incident impacting the confidentiality, integrity or availability of Norton Rose Fulbright Confidential Information, Supplier must:

i. Without undue delay and within forty-eight (48) hours of the security incident being detected, report the security incident to Norton Rose Fulbright using the contact information provided in this Standard; the delay is reduced to twenty-four (24) hours if it is established that the confidentiality, integrity or availability of Norton Rose Fulbright Confidential Information has been significantly compromised;

ii. Fully cooperate with Norton Rose Fulbright by providing all information relevant to the security incident in a timely manner;

iii. Fully cooperate with Norton Rose Fulbright to identify a root cause, remediate the security incident and make any notifications required by applicable law.

Compliance and Security Review Rights

13.1 **Regulatory compliance:** Supplier must comply with all requirements communicated by Norton Rose Fulbright that are imposed on Norton Rose Fulbright by government entities or regulatory agencies. Norton Rose Fulbright expects Supplier to provide necessary documentation in support of audits of Norton Rose Fulbright, upon Norton Rose Fulbright's request.

13.2 **Independent third party audits:** Supplier must periodically engage an independent third-party security company to audit and test Supplier's information security controls. Supplier must implement a process to resolve any risks or issues identified during these audits.

Upon request, Supplier will provide evidence of such audits results and actions taken to remedy any identified deficiencies.

13.3 **Right to audit:** The Supplier shall maintain complete, accurate and up to date records pertinent to the performance of the Supplier's obligations under the Agreement and retain them for six years from the termination or expiry of the Agreement. Without limiting the provisions of the previous paragraphs of this Standard, as a regulated entity Norton Rose Fulbright may require rights of access for Norton Rose Fulbright and its auditors (for example Norton Rose Fulbright's professional bodies or law enforcement agency) to carry out audit tasks which relate to the Agreement. The Supplier shall use reasonable endeavours to ensure access to premises, personnel, equipment and other support as reasonably required for such tasks. These record and audit right provisions will survive any termination of this Agreement.

Definitions applicable to this standard

Agreed Locations means the jurisdiction where Norton Rose Fulbright is established (and where this is England the Agreed Locations are the United Kingdom and the European Economic Area) and/or such other jurisdiction(s) agreed by Norton Rose Fulbright in accordance with the terms of this the Agreement or if none specified in the terms of the Agreement then such locations agreed in writing by Norton Rose Fulbright.

Agreement means the agreement between Norton Rose Fulbright and Supplier to which this Standard is appended or, if none, this Standard.

Norton Rose Fulbright means the Norton Rose Fulbright Entity procuring the Services.

Norton Rose Fulbright Confidential Information means all data or information in any format (including in written, oral, visual or electronic form) obtained by Supplier directly or indirectly from Norton Rose Fulbright or any other Norton Rose Fulbright Entity at any time relating to the Norton Rose Fulbright Entities or to the clients, customers, members, partners, personnel, business, finances, assets, operations, know-how, strategy or affairs of any of the Norton Rose Fulbright Entities, as the case may be, and any data or information required under or pursuant to this Agreement and which, in consequence of the negotiations relating to this Agreement or the exercise of its rights or performance of its obligations hereunder, acquired by or on behalf of the Supplier at the offices or other premises or through access to any IT systems of any Norton Rose Fulbright Entities or whether obtained through observations made by or on behalf of Supplier, including any information inadvertently acquired by Supplier while at Norton Rose Fulbright premises and whether before or after the date of this Agreement.

Norton Rose Fulbright Entities means the Norton Rose Fulbright Verein, the member firms from time to time of the Norton Rose Fulbright Verein (who, at the date of this Agreement include Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP, Norton Rose Fulbright South Africa Inc, Norton Rose Fulbright US LLP), and Norton Rose Fulbright Development Holdings Limited, Norton Rose Fulbright Australia Services Pty Ltd, Jaramer Pty Ltd , TNB & Partners, Services OR LP/SEC a limited partnership established in Canada, Shanghai Pacific Legal; and in every case their respective affiliates, associates or subsidiaries from time to time; and any references to **Norton Rose Fulbright Entity** will mean any of them as appropriate.

Services has the meaning given to it in the Agreement or, if none, the goods, works, services, functions and responsibilities agreed to be provided by Supplier to Norton Rose Fulbright including any incidental goods, works, services, functions and responsibilities reasonably and necessarily required for the performances of such services.

Supplier means the person providing the Services to Norton Rose Fulbright.