STORE DNA

Supplier / Employee

Information Security Requirements Policy

StoreDNA Information Security
Policy Owner: Dag Ainsoo
Approval date: 02 February 2018
Version: V1.1

TABLE OF CONTENTS

1. PURPOSE

StoreDNA (the Company) uses a number of suppliers and employees who provide services and goods. The effective management of these parties is essential in the provision of onward services to the Company's clients and ensuring the security of the Company's systems and data. The Supplier/Employee Information Security Requirements Policy (the Policy) describes control requirements for parties who manage secret or confidential information.

2. SCOPE

This Policy applies to all employees and suppliers which process, access, hold or transmit StoreDNA Protected Data.

3. PREFACE

Whilst it is the intention that both new and existing parties included in the above scope will be required to comply with this Policy, it is intended that existing parties will be assessed on a prioritised basis dealing with the largest and most significant first, ultimately with the aim to cover all.

All new Suppliers and Employees will be required to comply with the terms of this Policy. Suppliers of non-permanent staff (referred to as freelancers) fall under existing freelance recruitment procedures.

4. OVERVIEW

It is of vital importance to StoreDNA that its secret and confidential information remains secure and protected at all times. This Policy establishes the minimum standard for information security that should be applied by relevant Employees and Suppliers to StoreDNA on a global basis to protect StoreDNA resources and data.

5. DEFINITIONS

"Information Security Incident" means (i) the loss or misuse (by any means) of any StoreDNA Protected Data; (ii) the inadvertent, unauthorised and/or unlawful processing, corruption, modification, sale, or rental of any StoreDNA Protected Data; or (iii) any other act or omission that compromises the security, confidentiality or integrity of any StoreDNA Protected Data.

"Information Systems" means all hardware, software, operating systems, database systems, software tools and network components used by or on behalf of StoreDNA to receive, maintain, process, store, access or transmit StoreDNA Protected Data.

"StoreDNA Protected Data" means any data or information of or concerning StoreDNA or its Affiliates or StoreDNA's, or StoreDNA's Affiliates', Clients or other recipients of the Services that is provided to or obtained by Party or any member of Supplier Personnel in connection with the negotiation and execution of the Agreement or

the performance of Supplier's obligations under the Agreement, including any such data and information that either (i) is created, generated, collected or processed by Supplier Personnel in the performance of Supplier's obligations under the Agreement, including data processing input and output, Service Level measurements, asset information, reports, third party service and product agreements, and Supplier's charges to StoreDNA, or (ii) resides in or is accessed through StoreDNA's Information Systems or Supplier's Information System; as well as any data and information derived from the foregoing. For the avoidance of doubt, StoreDNA Protected Data includes, but is not limited to, all StoreDNA Secret and Confidential Information.

"Security Questionnaire" means the questionnaire designed to assess Supplier's information security controls in alignment with industry standards (ISO 27001/27002) that is provided by StoreDNA and completed by Supplier.

"Supplier Personnel" means any and all personnel engaged by or on behalf of Supplier to perform any part of the Services, including employees, freelancers and independent contractors of Supplier and Supplier's Affiliates.

6. COMPREHENSIVE INFORMATION SECURITY PROGRAMME

Supplier warrants and represents, on an on-going basis, that all answers provided by Supplier within the Security Questionnaire are accurate.

Supplier shall not materially change any aspect of the Supplier's operations that would, from the perspective of StoreDNA, degrade or otherwise materially adversely impact the level of security provided to StoreDNA Protected Data.

Supplier shall reassess against the Security Questionnaire upon the earlier of (a) any material change to any aspect of the Supplier's operations; or (b) every three years.

Where, as a result of any such reassessment, the Supplier's answers to the Security Questionnaire no longer accurately reflect the Supplier's operations, the Supplier shall promptly provide an updated Security Questionnaire to StoreDNA.

7. REMOTE ACCESS TO STORE DNA INFORMATION SYSTEMS

When remote access to StoreDNA systems is required, the Supplier will be provided with secure access to an email account, an external cloud based system and/or an StoreDNA laptop. Any changes on the supplier personnel accessing StoreDNA systems need to be notified to StoreDNA as soon as possible not exceeding 5 working days.

8. PROTECTING STORE DNA INFORMATION

Supplier shall implement agreed as well as general information security best practices across all supplied components and materials including software, hardware and information to safeguard the confidentiality, availability and integrity of StoreDNA and its information. When applicable, the Supplier shall provide StoreDNA with full documentation in relation to the implementation of logical security and shall ensure that it has such security that:

- prevents unauthorised access to StoreDNA systems,
- reduces the risk of misuse of TSP systems or Information
- detects security breaches and enables quick rectification of any problems and identification of the individuals who obtained access and determination of how they obtained it.

9. DATA ENCRYPTION

Supplier will encrypt all StoreDNA Protected Data when stored on portable devices and media or when transmitted over non-secure communication channels (e.g. internet, email or wireless transmission) including remote connectivity using solutions that are certified against the U.S. Federal Information Processing Standard 140-2, Level 2, or equivalent industry standard, and will verify that the encryption keys and any keying material are not stored with any associated data.

When transferring StoreDNA Protected Data and in communications between StoreDNA and Supplier, Supplier will use secure email, such as enforced Transport Layer Security (TLS), and will implement any network connectivity with StoreDNA that Supplier is required to provide by StoreDNA in accordance with any StoreDNA-approved connectivity standards.

In the event that StoreDNA Protected Data could be transferred to removable media, a mobile device or uncontrolled computer, Supplier will implement, monitor and maintain encryption and information leakage prevention tools using solutions that are certified against the U.S. Federal Information Processing Standard 140-2, Level 2, or equivalent industry standard, and will verify that the encryption keys and any keying material are not stored with any associated data.

Supplier shall prohibit the transfer of StoreDNA Protected Data to Supplier mobile devices where the security measures employed on such mobile devices do not meet the requirements of this Section 9 (including, without limitation, where such mobile devices do not support the technologies required to comply with such requirements).

10. ACCESS

a) General

Supplier will limit access to StoreDNA Protected Data to authorised persons or roles, based upon a principle of least privilege which limits all users to the lowest permission levels that they can be assigned to that does not prevent the relevant Supplier Personnel from completing their assigned tasks.

Supplier must confirm the identities of all Supplier Personnel using independent, verifiable identity documents (for example, government-issued documents such as a passport or driver’s licence) prior to creating any accounts for Supplier Personnel that will provide access to the Supplier's Information Systems.

Supplier will review all account access and change such access commensurate with role

changes.

b) Passwords

Any passwords issued to a user by an administrator must be reset by the user upon initial use.

Where user-initiated password resets are used, the processes that create the temporary password must create secure temporary passwords which cannot be derived from previous passwords (for example, an auto-incrementing system which generates "abc1" followed by "abc2" would not meet this requirement nor would a system which identifiably uses the current date as the basis of password generation), must not reuse passwords and must communicate the temporary password to the user through a channel accessible only to the user.

Where Supplier suspects any unauthorised access has occurred to any user account, Supplier shall immediately revoke the password to such user account.

11. VETTING OF SUPPLIER PERSONNEL

Supplier shall ensure that any Supplier Personnel who will have:

a) physical access to any StoreDNA site for a period of time sufficient to warrant StoreDNA security providing such Supplier Personnel with an identification badge permitting unescorted access; or
b) access to StoreDNA Protected Data,

shall have been the subject of pre-engagement screening in accordance with Attachment A to this Policy.

12. PHYSICAL SECURITY

Depending on the type of services that the Supplier is providing, one of the following (a or b) controls will be required:

a. General
   Supplier shall ensure that StoreDNA Protected Data is physically secured against unauthorised access, including, but not limited to, by use of appropriate physical safeguards such as electronic ID card access to all areas of the Supplier's Information System.
b. Hosting
   Where, and to the extent that, Supplier is providing hosting services[1] as part of the Services, it must implement the following controls as a minimum level of physical security:
   - All hosting facilities including buildings and infrastructure shall meet the

[1] In the context of this policy, these physical controls for hosting services will only be applicable when Supplier hosts live services for the Company or its Clients. Typically Suppliers to the Company would only host development and/or test environments on their premises. Therefore, physical access should, as a minimum, follow a).

standards set out in ISO/IEC 27001 and also ISAE 3000 /3402 or such other standards agreed in writing by StoreDNA following a security risk assessment undertaken by StoreDNA or an independent third party.

- All StoreDNA Protected Data processed, accessed, held or transmitted by Supplier will be physically stored in a facility subject to the following security controls:
    - authorised access control list requiring a photo ID check to access data centre floor;
    - biometric and/or keycard access to monitored man-traps leading to data centre floor;
    - locked server cabinets;
    - 24x7 indoor and outdoor CCTV monitoring with video being saved for at least 30 days;
    - 24x7 physical intrusion monitoring alarm system;
    - roaming security guards; and
    - no windows are present on the data centre floor.

13. MALICIOUS CODE

Supplier will not incorporate or introduce or permit or facilitate the incorporation or introduction of Unauthorised Code into the Supplier's Information Systems nor any StoreDNA Information Systems.

Supplier shall ensure it at all times employs adequate security practices to prevent, detect, mitigate and protect against the introduction of any such Unauthorised Code into the Supplier's Information Systems in real-time.

“Unauthorised Code” is defined as any: (i) computer virus, harmful programmes or data that destroys, erases, damages or otherwise disrupts the normal operation of the Supplier's Information Systems, allows for unauthorised access to the Supplier's Information Systems, (ii) worms, trap door, back door, timer, counter, software locks, password checking, CPU serial number checking or time dependency or other such limited routine instruction that is designed to interrupt or limit the proper operation of the Supplier's Information Systems, (iii) spyware/adware, and (iv) any other similar programme, data or device that is being inserted for an improper purpose.

14. NETWORK SECURITY

On reasonable notice or information and during normal working hours, StoreDNA shall have the right, but not the obligation, to review periodically the Supplier's and/or Supplier Affiliates’ operations, processes and systems insofar as they relate to the Services for the purpose of monitoring the Supplier's and/or Supplier Affiliates’ compliance with the terms and conditions of these Information Security Requirements. Such reviews shall not relieve the Supplier and/or Supplier Affiliates from their responsibilities to comply with, and monitor its own compliance with, all terms and conditions of this Policy.

Supplier shall implement all recommendations resulting from any such audit having been

conducted.

Supplier shall maintain and keep up to date the network component inventories, network topology diagrams, data centre diagrams and IP addresses for each network that connects to StoreDNA Information Systems (and their interconnections), whether supported by the Supplier, any Supplier Affiliate or a third party on Supplier's behalf, to a standard that meets compliance requirements for all connectivity to the Supplier's Information Systems from the Internet, to include at least the following:

- ensuring the network perimeter is protected by industry-leading enterprise firewall systems, including (but not limited to): (i) establishing port, protocol and IP address restrictions that limit the inbound/outbound protocols to the minimum required; and (ii) ensuring all inbound traffic is routed to specific and authorised destinations;
- interrogating TCP protocol communications at the packet level to distinguish legitimate packets for different types of connections and reject packets that do not match a known connection state, i.e., stateful inspection. This must cover network, application and database protocols;
- configuring perimeter systems with redundant connections, to ensure there are no single points of failure;
- interrogating communications by monitoring network packets to identify and alert upon or prevent known patterns that are associated with security vulnerabilities or denial of service attacks with regularly updated signatures to generate alerts for known and new threats;
- maintaining and enforcing security procedures in operating the network that are at least: (i) consistent with industry standards for such networks; and (ii) as rigorous as those procedures which are in effect for other similar networks owned or controlled by Supplier;
- maintaining and enforcing operational and security procedures that prevent the provision of network connectivity to third parties where such access would enable the third party to access StoreDNA Protected Data, or access the StoreDNA Information Systems should network interconnections between StoreDNA and Supplier be enabled, without express written permission from StoreDNA;
- implementing perimeter management controls to ensure, at a minimum, that perimeter systems are configured to be resistant to resource exhaustion (e.g., to denial of service attacks); and
- keeping StoreDNA Protected Data logically separated from all other Supplier or Supplier customer data.

15. SECURITY INCIDENT MANAGEMENT

a) General.

Supplier will implement documented standards / procedures for dealing with suspected and actual security events, incidents and cybercrime attacks against the organisation (the “Incident Management Procedure”) and shall provide StoreDNA with full details of such Incident Management Procedure upon request.

b) Data Security Breach Reporting.

The Supplier shall notify StoreDNA of any suspected and actual security events, incidents and cybercrime attacks by emailing StoreDNA using the email address provided on MSA (clause 5.3).

Supplier will notify StoreDNA within six (6) hours of identifying an actual or potential Data Security Breach.

c) Data Security Breach.

In the event of a Data Security Breach, Supplier will:

- take all appropriate corrective action including, solely at the request of StoreDNA (and at the expense of Supplier where the Data Security Breach save where the Data Security Breach is due to the fault of StoreDNA), providing notice to all persons whose personal data may have been affected by such Data Security Breach, whether or not such notice is required by Applicable Law; and
- where the Data Security Breach is due to the fault of Supplier, reimburse StoreDNA (subject to StoreDNA giving Supplier written notification of such costs together with reasonable supporting information) for all reasonable costs StoreDNA may incur in connection with remediation efforts, including costs incurred in connection with;

    (i) the development and delivery of legal notices as required by Applicable Law and as reasonably directed by StoreDNA where not required by Applicable Law;
    (ii) the establishment of a toll-free telephone number where affected persons may receive information relating to the Data Security Breach; and
    (iii) the provision of credit monitoring/repair and/or identity restoration for affected persons for one (1) year following the announcement or disclosure of the Data Security Breach or following notice to the affected persons, whichever is later, or such longer period as is required by Applicable Law.

- resolve any Data Security Breach resulting from unauthorised access, including identification of any StoreDNA Protected Data disclosure, alteration or loss, and notification of StoreDNA as required under the Incident Management Procedure.

Within five (5) days after detection of such a compromise, Supplier shall provide to StoreDNA a root cause analysis and written notice with confirmed receipt of such unauthorised access or modification. Such notice shall summarise in reasonable detail the impact of such unauthorised access or modification upon StoreDNA and as applicable the persons whose personal data is affected.

Supplier must remediate any Data Security Breach within fourteen (14) days of such a compromise resulting from unauthorised access, including identification of any StoreDNA Protected Data disclosure, alteration or loss, and notification of StoreDNA as required under the Incident Management Procedure. In the event the Supplier determines that a Data Security Breach cannot be remediated within fourteen (14) days, Supplier must submit and obtain StoreDNA's written consent to a remediation plan within seven (7) days of the Data Security Breach.

16. REPORTING

At StoreDNA's discretion and with due regard to the type of service provided, Supplier shall provide the following reports to StoreDNA at the frequency set out below:

Report (Examples)	Description	Frequency
Service Level Agreement (SLA)	Metrics which demonstrate achievements on supplier SLAs.	Quarterly
Joiners, Movers and Leavers	Report users which need to be added or deleted from StoreDNA systems.	Movers and Leavers within 5 days. Joiners – per request

17. INDEMNITY

The Supplier shall indemnify, defend and hold harmless StoreDNA and its Affiliates and StoreDNA's or its Affiliates Clients and the officers, employees, sub-contractors and agents of any of them against all and any actions, costs, claims, losses, damages, expenses and liabilities of whatever kind made relating to or arising out of the breach by Supplier of the terms of these Information Security Requirements.

18. AUDIT

On reasonable notice or information and during normal working hours, StoreDNA shall have the right, but not the obligation, to review periodically the Supplier's and/or Supplier Affiliates' operations, processes and systems insofar as they relate to the Services for the purpose of monitoring the Supplier's and/or Supplier Affiliates' compliance with the terms and conditions of this Policy. Such reviews shall not relieve the Supplier and/or Supplier Affiliates from their responsibilities to comply with, and monitor its own compliance with, all terms and conditions of this Policy.

Supplier shall implement all recommendations resulting from any such audit having been conducted.

Attachment A
Pre-Engagement Screening

1) Screening of Supplier Personnel and/or New Employees

a) Screening.

Supplier shall perform the pre-engagement screening of Supplier Personnel at the time of hiring the Supplier Personnel in a manner that is consistent with StoreDNA's minimum required screening criteria as set forth within this Attachment and as permitted by law in the country of hire.
In addition, where permitted by local law, StoreDNA or its designated agents may perform additional screening relating to identity, criminal record and debarment of any Supplier Personnel.

b) Cooperation.

Supplier agrees to cooperate with StoreDNA in connection with such screening by requiring Supplier Personnel to submit information reasonably required to enable StoreDNA or its agents to identify such personnel and conduct such screening. Should any Supplier Personnel refuse to cooperate with such screening, Supplier shall not use that person to provide the Services unless specifically approved by StoreDNA.

Supplier shall be responsible for maintaining a pool of pre-screened personnel as reasonably necessary to support Supplier's performance of the Services.

c) Minimum Required Screening

- An identity check.
- Verification of entitlement to employment through the use of work permits or similar documents.
- Verification of pertinent licences including, motor vehicle licences, certifications and operating documents that are required by law or required due to the nature of the position/job description and/or responsibilities.
- Previous employment reference check.
- Verification of dates of employment claimed for the previous five (5) years.

d) Staffing Standards.

Supplier shall not permit any person to perform the Services who has been identified as:

- previous employment with StoreDNA that was terminated with cause;
- false statements or claims on CV/resume/application forms;
- false or exaggerated educational or professional qualifications;
- inappropriate references from referees or previous employers;
- relevant and/or undisclosed criminal convictions (where are allowed by law);
- unexplained gaps in employment history;
- lack of co-operation by the applicant; or
- exclusion by federal government.

In addition to Supplier's obligations pursuant to this Section, Supplier shall use reasonable judgment, on a case-by-case basis, based on the results of such screening, when evaluating whether any Supplier Personnel should be involved in the provision of the Services given the nature of the Services to be performed by such Supplier Personnel.