DFS Information Security Requirements for Business Partners

The Business Partner recognizes that security is a fundamental consideration for DFS and that the Business Partner's compliance with security requirements set forth herein is an obligation that is essential for DFS to consent to the Agreement.

DEFINITIONS

Business Partner: Suppliers including, but not limited to service providers, distributors, manufacturers, landlords, as well as any third party which has a relationship with DFS.

Data: All content and data including personal data and confidential information (i) transmitted or made available by DFS and/or its affiliates or on behalf of the DFS and/or its affiliates to the Business Partner, (ii) collected by the Business Partner through the services, as well as (iii) all data generated, handled or modified by the Business Partner as part of the services.

Data Breach: Any event leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Client's Personal Data, by any third party (including another Affiliate). A Data Breach is a Security Incident.

Good Industry Practice:

In relation to any undertaking and any circumstances, the exercise of that degree of professionalism, skill, diligence, prudence and foresight which would be expected from a skilled and experienced person, or an internationally recognized Company engaged in the same type of activity under the same or similar circumstances. The Good Industry Practices include for instance the respect of international norms and standards such as National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI-DSS), ISO27001, China's Multi-Level Protection Scheme (MLPS).

Security Incident: Any event impacting or likely to impact the security of the Data in terms of availability, integrity, confidentiality and traceability or any other event which may be considered as a security incident under the applicable data protection legislation and/or applicable cybersecurity standards.

REQUIREMENTS FOR ALL BUSINESS PARTNERS

1. Governance, Policy, and Regulations on Information Security

The Business Partner shall take into account the sensitivity of the Data at stake and potential risks in order to determine the appropriate security measures to be taken and to limit the likelihood of the risks to an acceptable level. These security measures shall in any event be consistent with the state-of-the-art and the rules of Good Industry Practices.

Any major change to these measures that may negatively affect DFS, and the Data shall be documented and notified to DFS.

The Business Partner undertakes to implement measures to ensure the confidentiality, integrity, availability, and traceability of the Data and the maintenance of an up-to-date documentation describing the technical and organizational security measures implemented to this end.

2. Authorized Use

The Business Partner shall implement and maintain an internal acceptable use policy, in which it will inform all its personnel of their responsibilities and will ensure their compliance.

The Business Partner shall ensure the Data is accessible only for the Business Partner's personnel and sub-contractors who are duly entitled and authorized, on a need-to-know basis, within the strict limit of what is needed to perform their duties.

3. Roles and Responsibilities

The Business Partner shall define the internal roles and responsibilities of the Business Partner's personnel and sub-contractors who are duly entitled and authorized in relation to information security.

4. Training and Awareness

The Business Partner shall provide all personnel (including current employees, new hires, and transfers) information security training and awareness appropriate to their roles and responsibilities.

5. Information Security Incident Management Process

The Business Partner implements measures to detect, resolve and notify DFS of Security Incidents and Data Breaches within the time limits required by applicable data protection legislation.

Without any limitations of DFS other rights and remedies, in case of any actual or reasonably suspected Security Incident, the Business Partner shall notify DFS without undue delay after becoming aware of such actual or suspected Security Incident, and in any case in accordance with applicable data protection legislation, by email at the following address cybersecurity@dfs.com.

Immediately following such notification, the Business Partner shall investigate the Security Incident and provide DFS with regular updates regarding its handling of the matter.

The Service Provider shall take appropriate steps, to (i) remedy the Security Incident, (ii) mitigate its effects and (iii) make any appropriate changes to prevent such Security Incident from recurring. The Service Provider will in addition assist DFS in restoring the Data.

6. Information Asset Management

The Business Partner shall keep an accurate and complete inventory of computer hardware and software assets that are used to process DFS data from acquisition to retirement or withdrawal.

The Business Partner must ensure assets that storing DFS information shall be separated from other clients.

7. Network Security

The Business Partner will ensure that all its computer systems and the ones of its subcontractors that are used for the services provided to DFS are protected against of threats and attack within the Business Partner's network (and of any relevant subcontractor). The Business Partner and its subcontractors shall take the following protection mechanisms (as appropriate):

a. Network Access Control to limit access only to those authorized personnel.
b. Restricting and filtering systems connection to the network
c. Encrypted wireless access only available to the authorized users.
d. Segregation of networks system

e. Remote access to a network to DFS Data

8. Monitoring

The Business Partner ensures that an adequate level of IT infrastructure monitoring capacity is implemented to detect possible information incidents or problems.

The Business Partner ensures the traceability of any operations (log records) performed on the Data. The logs must record user activities, exceptions, faults and other key events and be appropriately protected.

9. Protection Against Malicious Programs

The Business Partner will take all the necessary precautions to prevent the introduction of any malicious programs into DFS IT/IS systems and will take the appropriate measures (including diagnostic and restoration of the IT/IS systems and of the Data) should it detects the existence of such malicious programs.

10. Access Control Management

The Business Partner ensures that access to the Data will be restricted based on the data classification and associated risks, considering principles of need-to-know, least privilege and segregation of duties.

11. Authentication

The Business Partner implements and maintains policies and procedures to control logical access to the Systems and Data.

The Business Partner defines appropriate access rights and restrictions to the access of the Data.

The Business Partner ensures that strong authentication is equipped for privileged access to servers, applications, database, systems hosting the Data.

12. Physical Access to Facilities

The Business Partner defines and implements controls for physical access to its facilities, especially to places where the equipment that supports the information systems is located. Access records shall be periodically reviewed.

13. Secure Development Lifecycle

If the Business Partner engages in activities of developing system for DFS, the Business Partner implements and maintains a secure development lifecycle management policy including:

- using secure coding practices and secure environments.
- developing in specialized development environments, isolated from the production environment, and protected against disruption and disclosure of information.
- carrying out system development activities (including coding and package customization) in accordance with security architecture, performed by competent experts and monitored in order to identify unauthorized modifications or changes which may compromise security.
- going through an official and documented revision and approval process Before the new systems are deployed in the production environment.

14. Change Management

The Business Partner shall establish standardized change management procedures. Changes to systems, from the early design stages through all subsequent maintenance efforts, must be subject to change management procedures.

The Business Partner shall communicate with DFS in advance when the change may have an impact on DFS.

15. Cryptography

The Business Partner implements cryptographic solutions meeting DFS' minimum encryption requirement of 128-bit AES and 256-bit SHA whenever applicable.

The Business Partner ensures the cryptographic keys in use are protected against unauthorized access or destruction.

16. Vulnerability Management

All critical vulnerabilities that could affect DFS systems, the Data or the services that the Business Partner provides to DFS and whose risk the Business Partner is planning to accept must be immediately communicated to DFS. The decision to accept the risk must be agreed upon in writing.

17. Security Assessment

Without prejudice to the ability for DFS to perform audits the Business Partner shall regularly control the conformity and adequacy of its technical and organizational security measures and be in a position to demonstrate their actual implementation and effectiveness, as well as its compliance with the requirements set forth in this document and its own security policies, by submitting its IT/IS systems to regular tests and audits.

18. Cloud Computing

If the use of cloud computing services (e.g., cloud type like public/private/community/hybrid, and cloud service types like Software as a Service (SaaS)/ Platform as a Service (PaaS) / Infrastructure as a Service (IaaS)) is necessary for the performance of the agreement with DFS, the Business Partners ensures that cloud security controls are a set to protect cloud environments against vulnerabilities and mitigate the effects of Security Incidents.

19. Authorized Subcontractors

Subject to DFS authorizing the use of subcontractors by the Business Partner, the Business Partner shall use only sub-contractors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing of Data will meet the requirements set under this document. The Business Provider shall check regularly, notably through audits, compliance of its own sub-contractors with the above-mentioned obligations.

20. Continuity of Service

The Business Partner shall implement and maintain, and shall cause each of its sub-contractors involved in the services to implement and maintain, business continuity policies and procedures in accordance with Good Industry Practices.

21. Right to Audit

For the duration of the agreement, the Business Partner authorizes DFS to conduct, or arrange to be conducted by independent auditors, prior written notice at least 10 business days in advance, – tests or audits of all or some of the services, including when performed by sub-contractors, to verify whether the Business Partner has complied with its obligations included in this document. The Business Partner will also allow DFS to carry out an inspection immediately after a Security Incident.

A report of such audit shall be sent to the Business Partner.

In case the audit report or any other security tests conclude that the security measures are not appropriate or sufficient, or reveal vulnerabilities or non-compliances with the requirements set forth in this document and/or Good Industry Practices, the Business Partner shall implement corrective actions within a period of time to be agreed by the parties depending on the seriousness of the breach, without prejudice to any additional rights of DFS.

22. Consequences of Termination of Service

The Business Partner undertakes, at the request of DFS and in any event following the termination or expiration of the agreement, to:

- return the Data to DFS in a readable and interoperable format within thirty (30) days as from such request or termination or expiration of the agreement.
- after such return, destroy all copies of the Data it may have in its possession. Such destruction must consist in irreversible deletion of all copies of the Data (including backups) on its equipment or on any other media in its possession, regardless of the medium (except if there is a legal obligation to store the Data).