SWIFT SECURITY MEASURES

This document describes the technical and organizational measures implemented at Swift to ensure an appropriate level of security for personal data, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. These measures are described in terms of objectives, for which specific controls have been defined and implemented.

1. Risk identification and management

- A governance structure is in place to identify and manage risks and monitor the effectiveness of risk management processes
- Risks related to critical suppliers are documented and managed

2. Information security

- Changes are planned, validated and authorised prior to implementation
- Cryptographic methods are designed and used to protect the confidentiality of customers' messages (both in transit and at rest)
- Customer authorised configuration changes are validated and implemented in accordance with the requests
- Mechanisms are in place to prevent and detect corruption of messages
- Only authorised customers can access messaging services and messages are delivered to authorised recipients only
- Physical access to premises, computer equipment and resources is restricted
- Security measures (including logical access) to protect confidentiality and integrity of data are implemented
- Swift processes personal data of its customers in line with documented service commitments
- Swift manages and monitors the Swift owned infrastructure at the TIPS Operator to meet documented service commitments

3. Reliability and resilience

- Availability of the messaging services are monitored to detect and react to problems

- In the event of an outage, policies, procedures, and resources are in place to support the timely resumption of services in line with documented service commitments
- Processes and procedures are in place to evaluate current processing capacity and use of system components to forecast capacity demand
- Swift has developed Business Continuity Plans and Disaster Recovery Plans in line with service commitments
- Swift validates messages and only validated messages are processed and delivered
- The messaging service infrastructure is designed to ensure the continuity of operations in line with documented service commitments

4. Technology Planning

- Vendor technology is evaluated before first use and during its lifecycle

5. Communication with users

- Customers are provided product and service information to support them in understanding and managing their risks
- Problems reported by customers are tracked, monitored and resolved in line with committed service levels
- Roles and responsibilities between Swift and its customers are in line with documented service commitments

6. Certification

- ISO27001 Certification
- PCI-DSS certification