SURE TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF PERSONAL DATA

Business continuity and disaster recovery

1 Definitions

"**Agreement**" means the relevant agreement entered into between any or all of Sure (Guernsey) Limited, Sure (Jersey) Limited, Sure (Isle of Man) Limited and Foreshore Limited with a Customer pursuant to which Sure acts a data processor.

"**BCMS**" means business continuity management system namely, part of the overall management system using an industry recognised method which implements, operates, monitors, reviews, maintains and improves business continuity as set out in paragraph 2(a) of this document.

"**BIA**" means business impact analysis namely, the process of analysing activities, processes, methods, dependencies of all parts of the business and the effect that a business disruption might have over time.

"**Business Continuity Plan**" means documented procedures that guide organisations to respond, recover, resume and restore to a pre-defined level of operation following disruption.

"**Customer**" means a customer of Sure who is party to an Agreement.

"**Policy**" means the key document that sets out the intentions and direction of an organisation as formally expressed by its Top Management.

"**Programme**" means the ongoing management and governance process supported by Top Management and appropriately resourced to implement and maintain business continuity management.

"**Sure**" means Sure (Guernsey) Limited, Sure (Jersey) Limited, Sure (Isle of Man) Limited and/or Foreshore Limited.

"**Top Management**" means person or group of people who direct(s) and controls an organisation at the highest level.

2 Business Continuity

(a) Sure has and will continue to have throughout the term of the Agreement, a BCMS that covers the systems storing Sure data.

(b) The BCMS will include, as a minimum, the following features:

1. A Policy;
2. A Programme;
3. A Business Impact Assessment process to create and maintain the Business Continuity Plans;
4. A Business Continuity Plan (or Plans) to minimise operational disruption to the provision of services.

(c) Sure will have the ability to implement the Business Continuity Plans (or Plans) without delay at any time.

(d) Sure will ensure that its suppliers needed to deliver services that it considers critical have appropriate Business Continuity Plans in place to prevent significant disruption to the services relevant to the fulfilment of Sure's obligations under an Agreement.

(e) Sure will provide, on request, high level details and information about its BCMS as part of any review required by the Customer and in the event that an issue is identified which may materially impact the provision of the services under the Agreement the parties shall use reasonable endeavours to rectify such issues.

3 Testing and Exercising

(a) Sure shall periodically test the effectiveness of its BCMS and Business Continuity Plans with relation to the provision of services to the Customer in accordance with the Customer's standard practices or as may be agreed by the parties.

(b) In the event that an issue is identified which may materially impact the provision of the services under the Agreement, the parties shall use reasonable endeavours to agree a plan to rectify such issues.

Part B:

Security

Part A

1. Sure shall comply and shall procure the compliance of its personnel and subcontractors, with the policy set out in Part B below and shall notify the Customer of any actual, potential or suspected breach of such policy.
2. Sure shall ensure that its security plan and/or policy fully complies with any applicable policy set out in Part B below.
3. Sure shall maintain adequate security controls and procedures in relation to the nature of its business.

Part B

Security by Design:

1. Secure Software Development Life Cycle (SDLC) is followed and can be evidenced.
2. Evidence of security checks and audits are carried out on the supply chain by or on behalf of providers of both third-party hardware and software elements used will be obtained where practical to do so.
3. System hardening is used to reduce vulnerabilities and threat landscape.
4. Systems provide functionality to restrict access based on network, transport and application level protocols.
5. Security awareness training and appropriate staff vetting is in place.
6. Security patches and updates are applied to Sure systems in a timely manner.

System Authentication Authorisation and Accounting (AAA):

1. Sure systems have had any default credentials including default usernames or passwords changed.

2. Sure systems do not rely on generic accounts — all logins (via GUI, direct OS, CLI, direct DB, API calls, etc.) are from uniquely identifiable and individually named accounts.
3. Sure systems, where technically possible, provide the capability to interact with remote authentication systems via standard methods such as LDAPS or SAML.
4. Sure systems where technically possible support strong authentication such as complex passwords and two-factor authentication.
5. Sure systems provide configurable role-based access control.
6. Authentication credentials are not hard coded into configuration files or scripts.
7. Sure systems provide logging capability for both system and user logging activities.
8. Remote logging is supported by Sure corporate systems. The logging format is standardised (for example remote syslog) and is ingested by leading SIEM tools.
9. Sure systems supports secure monitoring protocols such as SNMP v3, including the ability for default SNMP community strings and/or authentication details to be changed from default.

Data Security:

1. Traffic carrying sensitive or privileged data (e.g. management traffic or authentication requests) will always be sent over encrypted channels (SSH, TLS).
2. Any cyphers used meet best practice standards.
3. Sensitive data is not stored in program code.
4. Logs do not record sensitive data in plaintext.
5. Alarms do not contain sensitive data in plaintext.
6. Sensitive data is not transferred in plaintext in cookies of web applications.
7. Web applications submit sensitive data in HTCP-POST to prevent data disclosure.