ISMS 2
Business continuity plan

Public edition - business and personal information redacted

Document information			
Document name:	ISMS 2 Business continuity plan	**Document ID:**	ISMS 2
Document version:	1.0	**Date of approval:**	2020-01-13
Approved by:	CTO	**Revision interval:**	At least annually
Document owner:	Director of information security	**Information classification:**	Public
Reference:	ISO/IEC 27001		

Revision History

Author	Version	Date	Description
Director of information security	1.0	2020-01-13	First public version

Table of Contents

Abbreviation and definitions

BCP	**Business Continuity Plan**
RTO	Recovery Time Objective
DIS	Director of Information Security
DRP	Disaster Recovery Plan
Management Team	Refers to staff reporting directly to CEO

1 Introduction

This document sets out the Business Continuity Plan (BCP) for Sinch. The purpose of a formal BCP is to ensure that in the event of a serious incident an emergency procedure is initiated so that Sinch can continue to provide services to Clients with minimal interruption.

A “serious incident” is defined as an event which renders normal operations either temporarily or permanently impossible. This could for example be the result of a major accident, an environmental disaster or a terrorist attack. Normal operations could be interrupted either because it is unsafe to enter buildings, or because travel restrictions are in place that prevent access to Sinch premises.

Whatever the reason, it is assumed that normal operations will be completely or partially suspended and an alternative solution to carrying on our normal business is required, such as a complete loss of one public or collocated datacentres. In addition, an effective communications process will also be required to alert staff, clients, suppliers and all other relevant parties to the situation.

“Business Continuity Management is a holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.”

BSI BS25999-1 Code of Practice for Business Continuity Management (predecessor of ISO 22301:2012)

2 BCP Management

2.1 Management Structure

The Business Continuity Plan will be managed by the BCP Sinch Department Units as in Section 3: Disaster Recovery Plans and overseen by the DIS (Directory of Information Security), VP Operations and the CTO.

The principal objectives of the Departments are to manage, update and test the Disaster Recovery Plans, and to take control of their area of operations of the companies in the immediate aftermath of a disaster and to manage the recovery plan. Two areas of the business are highlighted below for special consideration People &Facilities and PR & marketing.

2.2 Roles and Responsibilities

Responsibilities of the Departments:

- Has ultimate responsibility for their own departments BCP Plan
- Must ensure that the Departments are always fully represented and that the team is individually aware of their own responsibilities.
- Is responsible for ensuring that the BCP is tested regularly and that the company maintains a record of such tests.
- In the event of a major incident, is responsible for making the initial decision on enacting the BCP, in conjunction with the Operational Representatives. Responsible for keeping the Management Team appraised of the situation as part of the contact strategy.
- Ensures the staff carry out their individual roles throughout the period of the incident
- Responsible for getting the business back to normality as quickly as possible.

Responsibilities of the HR / Facilities:

- Holds ultimate responsibility for staff communications.
- Must ensure that the contact details for staff at all Sinch sites are on Sinch Hub and staff are reminded every 6 months to update this information.
- Is responsible for maintaining the HR & Facilities Disaster Recovery Plans, ensuring it is accurate and up to date.
- Is responsible for testing the HR & Facilities Disaster Recovery Plans and taking remedial steps as required.
- Advises the Departments on property/access issues that may require the plan to be invoked.
- In the event of a major incident, is responsible for ensuring the contingency site/s, if listed in the DR plan, are open and fully Operational.
- Ensures that each part of the HR & Facilities Disaster Recovery Plans has been completed and that any issues or concerns arising are escalated to the Departments.
- Following a major incident, will be responsible for ensuring the property is safe and fit for re-occupation

Responsibilities of the PR / Marketing:

- The primary responsibility of the PR is to create, update and manage the messages sent by the company to public and other audiences about the situation that caused the BCP to be invoked and the on-going measures being taken to implement it.
- This responsibility includes the distribution of the same or similar messages to the rest of the Sinch global network and affiliated companies.
- The principal media for these communications is the company websites, the BCP phone-in number, the Sinch email system (assuming it is operational), and the messaging system.

2.3 Training and Awareness

It is vital for the integrity of the Business Continuity Plan that an effective training and awareness programme is maintained, in order that all staff understand their roles and responsibilities if the BCP is enacted. An overview of the Sinch BCP programme is included as part of the Induction Programme for new starters.

The Departments are responsible for the technical Training and Awareness for all staff in their business.

As members of the Departments change it is the responsibility of the DIS/CEO/CTO to ensure that replacements are identified and provided with training on their specific role. It is also the responsibility of the Departments to train and brief BCP back-up members.

2.4 BCP Data and Documentation

Sinch's Business Continuity Data and Documentation is stored in the following locations:

1) Staff contact details are stored in the HR database Sinch Hub.
2) A list of staff mobile phone numbers (Business numbers & Personal if provided) is kept by HR in Sinch Hub. Staff are reminded every six months to check that contact information is up to date.
3) This document, the Sinch Group UK business Continuity Plan, and its Appendices are stored on Sinch SharePoint.

3 Business Continuity Strategy

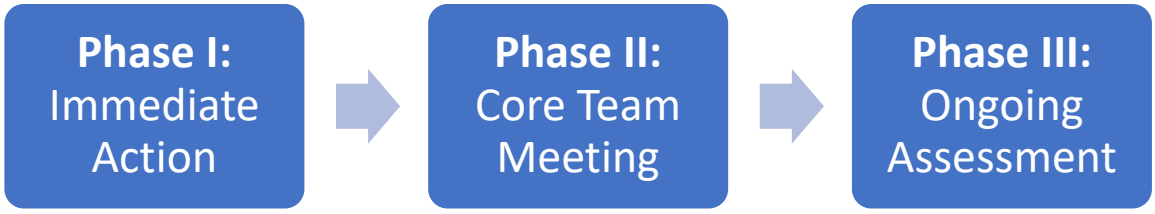
3.1 Overview

The Business Continuity Plan has been designed to be flexible in order that the Company can respond to a variety of different emergency situations. There are various scenarios that could be encountered, for example:

- Staff may not be able to travel to work as a result of travel restrictions (for example, in the case of a pandemic or alerts indicating a potential geographic health issue). NOTE: See section 4.
- Any building which needs to be evacuated as a result of bomb, fire, flooding or other incident, which make the building unsafe for staff to continue to utilise.
- The IT infrastructure ceases to operate as normal following a power shortage, cyber-attack, hardware failure or Internet failure.
- In order that the Business Continuity Plan can be enacted effectively, an initial assessment of the risk to the business caused by the emergency should be made by the Departments.
- The Departments will assess the needs of all teams and departments and ensure that the IT and Production teams invoke their disaster recovery plans appropriately. In most instances, priority should be given to the following departments: IT, Production and HR.
- The PR & HR team will then invoke the Communications Plan to keep staff, clients, suppliers and other stakeholders informed of the situation and what they should do as a result.
- The BCP response will be reviewed by the BCP Core Team at regular intervals and modified as appropriate. All decisions and actions taken will be documented, and the whole process will be reviewed once the emergency is over.

3.2 Enacting the Business Continuity Plan

The Departments will react to an emergency using a three-phase process.



3.2.1 Phase 1 – Immediate action

Step 1: Departments assesses the situation with the two key Operational Representatives (HR/Facilities & PR/Marketing) and decides as to whether any of the disaster recovery plans should be invoked.

Step 2: The disaster recovery plans are activated as required by the Department.

Step 3: Department contacts Management Team and informs them of the situation, and what action is taking place.

Step 4: HR / Facilities invokes the Contact Strategy, involving the Department and Business Representatives and the BCP Managers as appropriate. Informs any key partners about the situation such as third-party property owners.

Step 5: PR / Marketing keeps clients, press and other Sinch companies informed of the situation. PR representative posts relevant messages on the Sinch website, telephone and e-mail hubs so that all staff and third parties can be kept informed of the situation.

3.2.2 Phase 2 – Post-incident meeting

Once all initial communication has been made the Department & Management Team meets to assess the situation and to develop the follow-up plan.

The follow-up plan should include an assessment of whether the situation will last one hour, one day, one week or more than one week. Depending on this assessment, different strategies will be drawn up for locating and maintaining means of communication to meet the needs of different departments, Departments, services, and third parties to ensure the continuation of the business and minimal economic loss.

3.2.3 Phase 3 – Ongoing assessment of the situation

The Department will convene in person or online and continually assessing the gravity and timescale of the situation, keeping all parties informed, and providing for all business-critical needs.

The Department will keep Management Team informed of progress of the situation.

The PR Representative will continue to keep Press and other Sinch offices informed of the situation.

The Department should continue to meet regularly to keep re-assessing the situation, monitoring the disaster recovery plans, and communicating with key stakeholders, until the emergency is over.

3.3 Standing down the Business Continuity Plan

Once the emergency is over, the Business Continuity Plan can be stood down. However, the following activities should be completed first:

Situation Documentation: all of the decisions made, and actions taken during the emergency situation should be reviewed and recorded in full.

Assess the effectiveness: the effectiveness of the Business Continuity Plan should be assessed, and improvements made if required.

Update the BCP: the BCP documentation should be reviewed in changes have been recommended, and if there have been changes to infrastructure, personnel or procedures as a result of the emergency incident.

It is the responsibility of the Department to ensure these actions take place.

4 Disaster Recovery Plans

4.1 Global health issues / Pandemics

Sinch are globally prepared for widespread health issues including Pandemics due to the technology we have built as our infrastructure and our non-dependence on physical office locations.

4.1.1 Loss of Human Capital

General staff including support and operations teams are able to work remotely and perform all required duties in the event of loss of human capital, this has been planned and tested and will be enacted by HR in the event of a situation.

4.1.2 Facility Closure

Systems that Sinch use have redundancy between multiple datacentres in US and EMEA. If there were a failure of primary site, secondary sites handle client's traffic at the same capacity.

5 Communications Plan

5.1 Communications Strategy

The aim of the Communications Plan is to ensure that staff and other stakeholders are kept informed of the situation if the BCP is enacted. The HR / Facilities Representative is responsible for enacting and managing the Communications Plan; it is the responsibility of the Department to maintain the flow of effective communication during the emergency.

This BCP assumes that most staff will work remotely (either at home or at alternative premises) in the immediate aftermath of an incident which results in the Sinch premises being unavailable, this is detailed in the HR / Facilities DR plan dependant on region and locality of the office.

It is therefore essential that an effective communication process exists which enables all staff to be contacted with information about the incident and what they should do.

The Communications Plan uses three methods of communication with staff:

- All staff will be contacted via e-mail, Teams, Slack, Phone or the messaging service.

5.2 Contact Lists

Staff, clients, suppliers and other stakeholders may all need to be contacted in an emergency. To this end, the following contact lists are maintained in the locations indicated: See, Department DR Plans (Section 4)

5.3 Regular communications activities

In order to keep the contact lists up to date, the following actions must take place:

Contact List	Action and Frequency
BCP Department	Review with any business change or when enacted
Sinch Staff	Staff 6-month (automated) review of contact details
Clients	Sinch Status is a live system
Suppliers	Review with any business change

6 Maintenance and Testing

6.1 Maintaining the BCP

Maintaining the BCP documentation is critical to the success of a BCP deployment as under these circumstances staff must have immediate access to accurate information. Maintenance of the BCP documentation is the responsibility of the Departments.

BCP Core Members	Responsible For	Action and Frequency
Departments	Overall integrity of documentation	Review with any business change or when enacted. Minimum review period 12 months.
HR / Facilities	HR / Facilities DR Plan	Review plan with any business change or when enacted. Minimum review period 12 months.

6.2 Testing the BCP

Key components of the BCP are tested regularly, as follows:

- The internal staff messaging systems such as Teams, Slack, email & SMS are continuously maintained and tested.
- Home working is possible for all Sinch offices and acquired companies.
- Current backups of the application software, operating systems, and data are intact and available at off-site storage facilities, see back up policy.
- Key staff identified in this document have been trained in their emergency response and recovery roles.
- All DRPs in this document are tested on a regular basis, Minimum of one desktop exercise should be carried out for all Departments annually.
- Document review, maintenance, and updates are performed on a regular basis to ensure a viable state of readiness. Minimum review period 12 months.

For detailed testing of each Department see the DR plans listed in Section 4.