# Security Annex for 2FA

## Additional Terms for Two Factor Authentication Service

## CONTENTS

## 1 GLOSSARY OF TERMS & DEFINITIONS

**"2FA"** means the technology involved in the provision of the Two Factor Authentication Services, this can include Hardware Devices, Software Devices and third party services;

**"2FA Administration Portal"** means an Internet portal that allows the Administrator, through a web browser, to perform administrative functions including, but not limited to, assigning and de-assigning Devices to End Users;

**"Administrator"** means any person the Customer designates to administer the Service by the Customer;

**"Authentication Node"** means any item of Customer Equipment that is configured to receive access requests from End Users and to forward same along with the End Users' credentials to 2FA for verification;

**"Device"** means Hardware Devices and Software Devices;

**"End User"** means the actual end user of the Service;

**"Event"** means when any monitored component of the Supported Software is not operating pursuant to its standard functionality, as identified by a Monitoring Agent and indicated by alerts on Interoute's monitoring systems;

**"Hardware Device"** means a hardware token which may incorporate firmware (such as a key-fob token);

**"Incident"** means an unplanned interruption to a Service or deterioration in the normal quality of a Service;

**"Incident Management"** means the Incident management Service provided by Interoute pursuant to this Annex to investigate an Event or Incident;

**"SLO"** means Service Level Objective, which is a specific target within the Service Level Agreement;

**"Software"** means (i) Software Devices; and/or (ii) all other software provided to Customer; and

**"Software Device"** means a software token installed on generic hardware such as a PC, mobile phone or personal digital assistant.

**"Two Factor Authentication Service"** means the internet based authentication service, that validates the credentials of End Users passed to by the Authentication Node, provided by Interoute on behalf of Interoute's third party supplier;

Any other terms in capital letters shall have the meaning set forth in Schedule 1.

## 2 SERVICE DESCRIPTION

The Two Factor Authentication Service uses 2FA secure Devices to access the Customer's network. In order to permit access to the Customer's resources or network, the End User must have their username, password and (if applicable) the Device in their possession.

### 2.1 PROVISIONING

Interoute will ensure the Devices are initialised for use on the Two Factor Authentication Service and will deliver any Hardware Devices to the Customer at a single delivery address outlined on the relevant Purchase Order. It shall be the Customer's responsibility to distribute Hardware Devices or any Software Devices to their End Users.

### 2.2 CUSTOMER SETUP

Interoute will create an account for the Administrator on the 2FA Administration Portal in order for the Administrator to add the Authentication Node details into the 2FA Administration Portal.

### 2.3 TECHNICAL SUPPORT

Interoute will provide a first line support service to the Administrator which shall include call logging only. Interoute shall provide the first line support service during Working Hours. All other support shall be provided by the third party supplier. Except as set out in this Agreement, Interoute shall have no further liability in relation to these Services.

### 2.4 ADMINISTRATOR RESPONSIBILITIES

For the avoidance of doubt, the Administrator is solely responsible for the following:

a. Managing profiles, permissions and other aspects in respect of setting up and maintaining End Users within the system;

b. Providing information and instructions to End Users to enable authentication using the Two Factor Authentication Service;

c. Unlocking, resetting and re-synchronising Devices;

d. Diagnosing and replacing faulty and broken or lost Devices;

e. Setting up and managing the operation of the Authentication Node(s);

f. Gaining usage reports from the 2FA Administration Portal.

### 2.5 DEVICES

2.5.1 Devices are provided to the Customer on an “as is” basis.

2.5.2 It is the responsibility of the Customer to satisfy itself that the Devices will function in the way required and with the equipment it wishes to use them on. Interoute does not support any issues that may be caused by the use of the Devices and will not deal with issues relating to them directly.

2.5.3 Software Devices are provided to the Customer directly by Interoute’s third party supplier.

2.5.4 Hardware Devices are provided to the Customer by Interoute.

2.5.5 The third party supplier validates the use of the Devices on the generally available versions of the operating systems as advised by Interoute.

## 3 VENDOR CHANGE

Interoute may from time to time change its third party supplier of these Services. Such change will not require the Customer’s consent except where such change is likely to have a material adverse effect on the Service Levels following its implementation.

## 4 CHARGES

### 4.1 CHARGES PAYABLE BY THE CUSTOMER

Charges for the Service comprise of an initial on-boarding Installation Charge, a Fixed Rate Charge and any additional Charges set out within the Purchase Order.

### 4.2 ADDITIONAL CHARGES

4.2.1 Unless otherwise agreed between the Parties in writing, any Additional Charges will be charged according to the Professional Service Charges.

4.2.2 In addition to clause 4.2.1 above, any additional work agreed outside of a Working Day, will incur Professional Service Charges calculated on an hourly basis.

## 5 SERVICE LEVELS

Further to the Service Levels set out within the Schedule 2 to which this Annex is appended, Service Levels are defined for the following Service performance measurements:

a. Two Factor Authentication Service Availability

### 5.1 AVAILABILITY

| Service | Availability SLO |
|---|---|
| **Two Factor Authentication Service** | 99.95% |

Interoute uses the following formula to calculate monthly Availability:

$$Availability\ in\ \% = \frac{(Minutes\ in\ Monthly\ Review\ Period - Service\ Unavailability)}{Minutes\ in\ Monthly\ Review\ Period}$$

For the purpose of Availability measurement, Service Unavailability excludes any Planned Outage.

### 5.2 SERVICE UNAVAILABILITY

The Two Factor Authentication Service is considered to be Unavailable where the 2FA Administrator Portal is not accessible by Administrator(s).

## 6 SERVICE CREDITS

### 6.1 CLAIMING SERVICE CREDITS

6.1.1 Failure to meet a Service Level Objective (SLO) for a Service entitles the Customer to claim Service Credits (subject to the exceptions set out herein and in Schedule 1). The Customer must provide to Interoute all reasonable details regarding the relevant Service Credits claim, including but not limited to, detailed descriptions of the Incident, its duration and any attempts made by Customer to resolve it. Interoute will use all information reasonably available to it to validate claims and make a good faith judgment on whether the Service Levels apply to the claim.

6.1.2 Unavailability of the Service cannot be used to claim failure of another Interoute service. Interoute shall not be responsible for any cross default.

6.1.3 Interoute is entirely dependent on agreement from our third party supplier that there has been an issue or service performance problem. Interoute is unable to recognise Service Credits against the SLO without the third party supplier agreeing the failure of the service to perform.

### 6.2 CALCULATION OF SERVICE CREDITS

Where Availability falls below target during any Monthly Review Period, the Customer will be entitled to Service Credits as follows:

| Availability for the Service during Monthly Review Period falling below target by: | Service Credits as % of the applicable 2FA Fixed Rate Charge |
|---|---|
| Up to 1% | 5% |
| 1% ≤ 2.5% | 10% |
| 2.5% ≤ 5% | 15% |
| More than 5% | 20% |

# 7 CUSTOMER RESPONSIBILITIES

## 7.1 TECHNICAL REPRESENTATIVES

The Customer must designate one or more qualified persons as their technical representatives and support points of contact with Interoute. These technical contacts can be updated online, by phone, or email and must be provided for both pre and post installation, and during Incident Management.

## 7.2 OTHER RESPONSIBILITIES

Customer undertakes that it shall:

a. report any Incidents or problems with the Services to the Customer Contact Centre as soon as such problems have been identified;

b. provide feedback on any Interoute maintenance approval requests passed to the Customer within the reasonable times specified within such requests;

c. do such other things and provide such information as Interoute may reasonably request in order for Interoute to provide the Service;

d. not initiate a penetration test without agreeing and complying to the current Interoute Penetration Test Agreement. In case a penetration test is undertaken and no respective Interoute Penetration Test Agreement was signed, Customer herby agrees that the Interoute Penetration Test Agreement is deemed to have been signed and that its stipulations bindingly apply.

# 8 SERVICE OPERATION

## 8.1 INCIDENT MANAGEMENT

8.1.1 Depending on the impact an Event or Incident has on the Service, each Event or Incident is categorized pursuant to paragraph 8.1.2 into one of three priority levels: priority level 1 (Critical), priority level 2 (Major) or priority level 3 (Standard).

8.1.2 Any Events or Incidents relating to a security incident which requires post-restoration investigation are considered out of scope for the Incident Management Service.

| Priority | Description | Hours of Operation | Response Time | Update Frequency |
|---|---|---|---|---|
| Critical (1) | • When the Service is Unavailable. | 24/7 | 30 minutes | 2 hours |
| Major (2) | • The performance of the Service is degraded, but it is still Available<br>• A system or component of the Service is not available and a temporary fix may be available. | Working Day | 2 hours | |
| Standard (3) | • Where there is not a critical need and no impact to the delivery or use of the Service. | | 4 hours | N/A |

If Interoute responds to and works on a reported Incident and it is subsequently found not to be an Incident with the Service then Professional Service Charges will apply.

## 8.2 EXCLUSIONS

Interoute acts as a reseller of the Two Factor Authentication Service only.

Interoute shall not be liable to the Customer for the direct support of End Users of the Service.

Should any issues with the Devices arise, the Customer must contact Interoute and Interoute will forward issues to the third party supplier.

Except as set out above, Interoute shall have no further responsibility and/or liability to the Customer in relation to the Two Factor Authentication Service.