# SOIL

# Special terms



**Version: May 2017**

## Content

# 1 Definitions and Abbreviations

In addition to definitions and abbreviations in the General terms section 1, the following shall apply to the Agreement with regard to the Services covered by these Special terms:

| Term | Definition |
|---|---|
| SOIL Core Operator | EPIM's Contractor responsible for provisioning of the SOIL Core service. |
| SOIL Service Provider | An enterprise approved by EPIM and allowed to for provisioning of SOIL connection and security services to User organisations. |
| SSP | SOIL Service Provider. |

# 2 Service

## 2.1 Description

SOIL is a private cloud collaboration network and provides the oil and gas industry on NCS with an alternative delivery channel for critical information not desirable to transfer or publish via the Internet from a security and/or stability perspective.

SOIL consists of a redundant SOIL Core, located in Norway, governed by EPIM. User organisations must connect to SOIL via one or more EPIM approved SOIL Service Providers (SSPs), where the SSPs have a similar role as the Internet Service Providers (ISPs) on the Internet. As further described in 6.1, SSPs also have additional responsibilities including but not limited to providing a mandatory central SOIL firewall service for all their SOIL customers.

Refer to www.epim.no/soil for extended definition of the intention of SOIL.



## 2.2 Access management

a) When the User organisation is granted access to SOIL by EPIM, the User organisation's organisation name is added to a list of approved companies, accessible for all EPIM approved SSPs.
b) The User organisation is responsible for tendering one or more SSPs for providing SOIL access services as further described in 6.1.
c) The User organisation's chosen SSP(s) is responsible for connecting the User organisation to SOIL.
d) For access criteria and on-boarding procedures refer to www.epim.no/soil.

## 2.3 Support

Refer to www.epim.no/soil for support directions and guidelines.

## 2.4 Service level

### 2.4.1 Availability

EPIM endeavours to make SOIL Core fully operational and available to User organisations at all times.

In addition to Maintenance windows of the SOIL Core as specified below, the User organisation's chosen SSP(s) will have additional Maintenance windows. Use of multiple SSPs can mitigate undesirable extra Maintenance windows, for purposes requiring very high availability.

### 2.4.2 Standard Maintenance window

The Maintenance window for SOIL Core shall be on the last Saturday of each month between 00:00 and 04:00 hours (Norway time). (I.e. during the night between Friday and Saturday).

## 2.5 Data management

SOIL is a network service. No data stored in SOIL.

# 3 Service fees

EPIM does not charge any Service fee for SOIL, as SOIL Core is financed by EPIM's Members.

User organisation cover all own cost associated with establishing and operating their SOIL access services provided by their chosen SSP(s).

# 4 Security

## 4.1 Security Policy

- SOIL is a private network for parties authorised by EPIM.
- SOIL shall be closed for public networks and Internet.
- All User organisations shall present themselves on SOIL using public IP addresses.
- Each User organisation is responsible for:
    - Ensuring that only authorised parties can access SOIL.
    - Controlling their SOIL usage in collaboration with the chosen SSP(s).
    - Ensuring that the SOIL network is protected against any damage or harmful attacks through their SOIL access in collaboration with the SSP(s) used.
- All software in use must be continuously updated to ensure the security is maintained.



## 4.2 Organisational requirements

The User organisation connected to SOIL must have:

- An information security policy approved by User organisation's management.
- A named security officer in the User organisation.
- A dedicated function in the ICT operation concerned with information security.
- Updated documentation of the User organisation's use of SOIL.
- Procedures in place for awareness training of own staff, and other staff capable of accessing the User organisation's SOIL connection.

## 4.3 SOIL network security barriers

The SOIL network includes certain main network security barriers as described below:

### 4.3.1 SOIL Firewall

A mandatory SOIL firewall service provided by the chosen SSP(s), in compliance with the requirements stated herein.

The User organisation is responsible for appointing one or more named individuals authorised to contact chosen SSP(s) for requesting changes to rules for the SOIL firewall.

The User organisation may put an extra firewall between the SSP's SOIL firewall and own network.

### 4.3.2 Network segregation

All use of SOIL, including access to applications and services on SOIL, shall comply with procedures designed to keep SOIL separate from other networks, especially the Internet, in order to keep SOIL secure from malicious activities and faults. User organisations shall refrain from any activity which may breach this security.
Network resources (servers, applications, routers etc.) should not be connected to both Internet and SOIL, unless extra barriers are implemented and maintained to avoid "short circuiting" SOIL and Internet.
Public IP addresses and segments, used on SOIL, must be reserved for the purpose and not used on Internet.

### 4.3.3 Patching and antivirus software

Relevant security patches must be implemented for all networking resources, operating systems and applications connected to SOIL.

Security patches must be implemented without undue delay.

All ICT equipment connected to SOIL by User organisation shall have effective and updated antivirus software. Antivirus software must be promptly updated when new updates are available from the supplier of the antivirus software.



### 4.3.4 Check of content (optional)

The SOIL firewall service, provided by chosen SSP(s), does not include check of content by default. The User organisation may request content checking, in the SOIL firewall, as an extra service from the SSP(s). The SOIL Core does not perform packet inspection, nor perform any kind of content filtering.

User organisations must use relevant antivirus and anti-spyware for continuously checking content for malicious code.

### 4.3.5 Controlled use of active code

User organisations presenting applications on SOIL, with use of active code/content must control and verify that the active code is free from virus and not manipulated. User organisations, who make such applications available to others, must guarantee that such applications do not distribute unauthorised components or other malicious code. User organisations therefore need to use relevant measures to check for malicious code.

## 4.4 Security and operational guidelines

EPIM will, distribute additional operational guideline documents, when required, to ensure the security level on SOIL is appropriate. These will either be made available on www.epim.no/soil or be distributed to the User organisation's Contract administrators. User organisation is required to implement the guidelines, and any updates, in due time.

# 5 Processing of personal data

SOIL do not store or process any data, and thereby no personal data either.

# 6 Termination

No requirements beyond General terms section 8, as no data are stored in SOIL.

# 7 EPIM's additional obligations

## 7.1 SSP's responsibilities

EPIM has agreements with each EPIM approved SSP, where the SSP provides SOIL access services to User organisations on behalf of EPIM. The agreement between EPIM and the SSP requires the SSP to deliver the following mandatory services to User organisations:

1) SOIL connection.
2) SOIL firewall.
3) SOIL routing.
4) Technical service desk and operation of the SOIL connections and services.
5) Redundant connections between the SSP and the SOIL Core nodes.
6) Collaboration with the other SSPs for fault isolation and resolution.
7) On EPIM's behalf the SSPs are responsible for collecting relevant information from the User organisation for administration and use of SOIL.

## 7.2 Audits

EPIM is responsible for reviewing the SSPs' configuration, processes and documentation involved in the delivery of access to SOIL for User organisations.



# 8 User organisation's additional obligations

a) The User organisation is responsible for tendering one or more SSPs for a suitable SOIL connection.
b) The User organisation is responsible for collaborating on a technical level with the chosen SSP(s).
c) The User organisation must appoint and maintain the necessary technical and administrative contacts, requested by the SSP(s), and inform the SSP promptly in case of changes in such staff.
d) The User organisation is responsible for providing relevant information, upon request from the SSP(s).
e) The User organisation should only publish applications and services on SOIL aligned with the intention of SOIL being an alternative delivery channel for services not desirable to distribute via Internet as further described in section 2.1.

# 9 Governance

The SOIL Reference Group, consisting of Member representatives, is the governing body for the SOIL service. Policies decided by the SOIL Reference Group is effectuated by EPIM and implemented practically by the SOIL Core Operator, the SSPs and the User organisation.

# 10 Change Log

Major reworked since the March 2016 version.