

A picture containing text, clipart

Description automatically generated

##### **Information Security**

##### **Supplier Due Diligence Questionnaire**

##### **Tier 2 Supplier**

##### Standard Supplier

##### This document applies to: Seetec Group

Document owner: Steve Wiggett – Head of Information Security

Document author: Steve Wiggett – Head of Information Security

Contents

[1.0 Scope 3](#_Toc96961255)

[2.0 Overview 3](#_Toc96961256)

[3.0 Minimum Information Security Standards (Guidance) 3](#_Toc96961257)

[3.1 Risk Management: 3](#_Toc96961258)

[3.2 Compliance: 4](#_Toc96961259)

[3.3 Administration and Access Management: 4](#_Toc96961260)

[3.4 Physical Security: 4](#_Toc96961261)

[3.5 Employment Security: 4](#_Toc96961262)

[3.6 Incident Management: 4](#_Toc96961263)

[4.0 Questionnaire 4](#_Toc96961264)

[5.0 Document Control 7](#_Toc96961265)

[5.1 Version Control 7](#_Toc96961266)

[5.2 Next Review Date 7](#_Toc96961267)

[5.3 Document Authorised 7](#_Toc96961268)

# 1.0 Scope

This document applies to all suppliers who are assessed as being a Tier 2 Supplier to Seetec, as per the Supplier Impact Assessment.

**Tier 2 - Standard Supplier**

A Tier 2 supplier would have access to Seetec assets or office locations such as a cleaning company or contractors who attend office/site location to conduct work such as a lighting or heating engineer.

This document ensures that Security risks and issues are included as part of the due diligence process and is supported by the Seetec Supplier Security Management Policy.

# 2.0 Overview

Seetec has many information assets of varied sensitivity up to and including participant / service user data subject to GDPR protection and Seetec’s Confidential classification, as well as cloud services, hardware, server, systems, applications and staff with access to such information.

Seetec utilises a risk based due diligence approach to manage risk identification and associated mitigating control measures when working with suppliers and third parties to preserve the confidentiality, integrity and availability of Seetec’s information assets.

This document defines the Information Security due diligence question-set appropriate to the particular service being provided, as determined by the Supplier Impact Assessment, and is to be submitted to Seetec as part of the supplier onboarding and due diligence process.

This document outlines the Minimum-Security Standards for Suppliers and Third Parties who Seetec have assessed as a Tier 2 Supplier.

**Suppliers are to complete the questionnaire at Section 4. If a question is deemed not applicable or relevant, please mark as such. As part of Seetec’s due diligence process, a review is conducted whereby it is acknowledged that some of the below standards may not be required or applicable, depending on the business relationship. This will be considered as part of the due diligence review. Any queries will be raised as part of the Seetec response.**

# 3.0 Minimum Information Security Standards (Guidance)

Tier 2 Suppliers (as per Section 1.0) are expected to meet the following minimum-security standards:

3.1 Risk Management:

* Maintain an Information Security Policy.
* Maintain a Data Protection Policy/Framework.
* Maintain a Risk Management Framework.
* Maintain a Supply Chain Risk Management Policy.
* Mandatory annual Information Security and Data Protection training.

3.2 Compliance:

* Registered with the ICO (if appropriate)
* Person nominated within the business for Information Security and Data Protection.

3.3 Administration and Access Management:

* Principle of least privilege is adhered to.
* A password policy is maintained.
* Users’ identity is confirmed prior to password resets.
* New passwords are issued securely and not via the internet in clear text.
* New passwords are required to be changed at first use when reset or first issued.

3.4 Physical Security:

* Physical security control measures are in place for secure internal areas including comms/server rooms.
* Visitors Process

3.5 Employment Security:

* Background checks and screening are conducted on all new permanent and temporary staff, contractors, and sub-contractors prior to employment.
* An Acceptable Use Policy is in place.
* All security measures are extended to sub-contracting companies to ensure their compliance with company policies.
* Non-Disclosure agreements in place.

3.6 Incident Management:

* A documented Incident Management Policy and Procedure are in place.
* All staff are trained in the incident reporting process.
* Reviews of all incidents are carried out to identify areas of security improvement required and mitigation plans are initiated with relevant accountability applied.

# 4.0 Questionnaire

**Suppliers are to complete this section and provide supporting evidence where appropriate.**

Some questions may not be applicable for your organisation, if this is the case simply place N/A in the answer box.

|  |  |  |  |
| --- | --- | --- | --- |
| **QUESTION** | | **ANSWER** | **COMPLIANT?** (Seetec Group use only) |
| **RISK MANAGEMENT** | |  |  |
| Do you maintain an Information Security Policy? | |  |  |
| Do you maintain a Data Protection Policy/Framework? | |  |  |
| Do you maintain a Risk Management Framework? | |  |  |
| Do you maintain a Supply Chain Risk Management Policy? | |  |  |
| Are all staff required to complete mandatory Information Security and Data Protection training on an annual basis? Are compliance rates measurable? | |  |  |
| **COMPLIANCE** | |  |  |
| Do you hold any Information Security industry recognised certifications such as ISO27001, Cyber Essentials, Cyber Essentials Plus, SOC2 Compliance? | |  |  |
| What is your ICO registration number? | |  |  |
| Who is responsible for Information Security and Data Protection within your organisation? Please provide full name, email and contact telephone number | |  |  |
| **ADMINISTRATION AND ACCESS MANAGEMENT** | |  |  |
| Are all user accounts with access to the company network and systems/information that will be used for the processing, storage and transmitting of Seetec information given access based on the principle of least privilege only? | |  |  |
| Is a password policy maintained for all systems with minimum standards applied? | |  |  |
| Are users’ identities confirmed prior to password resets? | |  |  |
| Are new passwords issued securely and not via the internet in clear text? | |  |  |
| Are new passwords required to be changed at first use when reset or first issued? | |  |  |
| **PHYSICAL SECURITY** | |  |  |
| Have additional physical security control measures been put in place for secure internal areas including comms/server rooms? | |  |  |
| Are visitors logged in and out of all secure premises? | |  |  |
| **EMPLOYMENT SECURITY** | |  |  |
| Are background checks and screening processes conducted on all new permanent and temporary staff, contractors, and sub-contractors prior to employment? | |  |  |
| Is an Acceptable Use Policy in place? | |  |  |
| Are all security measures extended to sub-contracting companies to ensure their compliance with company policies? | |  |  |
| How do you ensure staff are aware of the non-Disclosure agreement and their responsibilities if on a Seetec site? | |  |  |
| **INCIDENT MANAGEMENT** | |  |  |
| Do you have a documented Incident Management Policy and Procedure in place? | |  |  |
| Are all staff trained in how to report a security incident? | |  |  |
| Are reviews of all incidents carried out to identify areas of security improvement? | |  |  |
| Named of Company Completing Form | |  | |
| Name of Person Completing Form | |  | |
| Declaration | I declare that the information provided in this questionnaire is true to the best of my knowledge and beliefs. | Signed:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Date |  |  |  |

# 5.0 Document Control

This is the change history and sign off information

## 5.1 Version Control

|  |  |  |
| --- | --- | --- |
| **Record of Amendment** | | |
| **Version Number** | **Date of Issue** | **Detail of Change** |
| V1.0 | 07/02/2022 | New document created |

## 5.2 Next Review Date

The next scheduled review of this document will be: February 2024

## 5.3 Document Authorised

|  |  |
| --- | --- |
| **Document Owner & Document Author** | |
| **Document Owner and Author:** | Steve Wiggett  Head of Information Security  Authorised: 28th February 2022 |