****

**GDPR Roles, Responsibilities**

**and Authorities**

Contents

1 Introduction 7

2 Information Security Roles 8

2.1 Organization Chart 8

3 Specific Role Responsibilities 10

3.1 Information Security Steering Group 10

3.1.1 Members 10

3.1.2 Responsibilities 10

3.1.3 Authorities 11

3.2 Information Security Manager 11

3.2.1 Responsibilities 11

3.2.2 Authorities 12

3.3 Information Security Administrator 12

3.3.1 Responsibilities 12

3.3.2 Authorities 12

3.4 Information Asset Owner 13

3.4.1 Responsibilities 13

3.4.2 Authorities 13

3.5 Information Security Auditor 13

3.5.1 Responsibilities 13

3.5.2 Authorities 13

3.6 Data Protection Officer 14

3.6.1 Responsibilities 14

3.6.2 Authorities 14

3.7 Customer Information Security Administrator 15

3.7.1 Responsibilities 15

3.7.2 Authorities 16

4 Other Roles with Information Security Responsibilities 17

4.1 Department Managers 17

4.1.1 Responsibilities 17

4.1.2 Authorities 17

4.2 IT Technicians 17

4.2.1 Responsibilities 17

4.2.2 Authorities 18

4.3 IT Users 18

4.3.1 Responsibilities 18

4.3.2 Authorities 18

**List of Figures**

[Figure 1 - Organization chart 8](#_Toc484526606)

# Introduction

Defradar Technologies treats the security of its personal data very seriously. One of the key attributes of an effective approach to information security is a clear allocation of roles, each with defined responsibilities and authorities. Each of these roles needs to be allocated to specific individuals or groups within the organization.

It is vital that everyone within the organization understands the part they must play in keeping the information we hold and process about individuals safe. This document should be read in conjunction with others that set out how information security is managed within Defradar Technologies, including:

* *Privacy and Personal Data Protection Policy*
* *Data Protection Impact Assessment Process*
* *Information Security Incident Response Procedure*
* *Personal Data Breach Notification Procedure*
* *Data Subject Request Procedure*

By ensuring that roles, responsibilities and authorities are clearly defined we will be in a good position to prevent many information security incidents affecting personal data from happening and to react effectively and appropriately if and when they do.

# Information Security Roles

Within the information security framework relevant to our compliance with the GDPR, the following major roles need to be defined and allocated:

* Information Security Steering Group
* Information Security Manager
* Information Security Administrator
* Information Asset Owner
* Information Security Auditor
* Data Protection Officer
* Customer Information Security Administrator (CSPs only)

The specific responsibilities and authorities of each of these roles are set out in later sections of this document.

There are also particular information security responsibilities that must be carried out by existing internal roles within the organization and these are also set out in summary within this document.

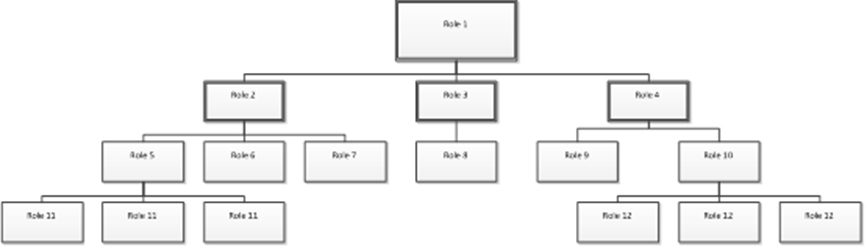
These roles are:

* Department Managers
* IT Technicians
* IT Users

In general, responsibilities that apply to all employees, contractors and other interested parties are set out within the relevant organizational policies.

## Organization Chart

A subset of the organization chart showing the relevant information security roles is shown below.



*Figure 1 - Organization chart*

# Specific Role Responsibilities

This section details the specific ***information security*** responsibilities and authorities of each role within the organization structure. It does not include any other types of responsibility e.g. managerial, technical and should not be taken as a full job description. Competences necessary to fulfil each role are defined in the document *Information Security Competence Development Procedure*.

## Information Security Steering Group

The Information Security Steering Group oversees compliance with the GDPR and the operation of information security controls as a representative of top management within and has overall responsibility for its effectiveness.

### Members

The group is made up of members of the top management team and will as a minimum include the following roles:

* Chief Operating Officer (COO)
* Chief Financial Officer (CFO)
* Chief Information Officer (CIO)
* Chief Privacy Officer (CPO)
* Information Security Manager

Further members may be nominated by existing members on an as-needed basis.

### Responsibilities

The Information Security Steering Group has the following responsibilities:

* Maintain a clear and current understanding of the GDPR legislation and its implications for the business processes of the organization
* Establish and maintain the information security policy, objectives and plans
* Communicate the importance of complying with the GDPR, meeting the objectives and the need for continual improvement throughout the organization
* Maintain an awareness of business needs and major changes
* Ensure that information security requirements are determined and are met with the aim of minimizing risk and maintaining effective controls for Defradar Technologies and for our customers
* Determine and provide resources to plan, implement, monitor, review and improve information security and management e.g. recruit appropriate staff, manage staff turnover
* Oversee the management of risks to the organization and its services
* Conduct management reviews of information security, at planned intervals, to ensure continuing suitability, adequacy and effectiveness
* Select auditors and ensure that internal audits are conducted in an objective and impartial manner
* Establish a continual improvement policy with respect to information security for Defradar Technologies
* Review major information security incidents
* Ensure that arrangements that involve external organizations having access to information systems and services are based on a formal agreement that defines all necessary security requirements

### Authorities

The Information Security Steering Group has the authority to:

* Approve significant expenditure on information security-related matters
* Recruit additional resources for the management of information security
* Approve high-level policies for information security
* Initiate high-level incident management actions

## Information Security Manager

The Information Security Manager is the primary role with a dedicated focus on information security and related issues.

### Responsibilities

The Information Security Manager has the following responsibilities:

* Reporting to the Information Security Steering Group on all security related matters on a regular and ad-hoc basis when required
* Communicate the information security policy to all relevant interested parties where appropriate, including customers
* Implement the requirements of the information security policy
* Manage risks associated with access to the service or systems
* Ensure that security controls are in place and documented
* Quantify and monitor the types, volumes and impacts of security incidents and malfunctions
* Define improvement plans and targets for the financial year
* Monitor achievement against targets
* Establish and maintain a continual improvement action list
* Report on improvement activities
* Identify and manage information security incidents according to a process
* Attend management review meetings on a regular basis
* Liaise with Cloud Service Customer representatives on information security-related matters

### Authorities

The Information Security Manager has the authority to:

* Declare information security incidents
* Approve limited expenditure on information security-related matters
* Review the operation of controls within all business areas

## Information Security Administrator

The Information Security Administrator is a technical role involved in the implementation and maintenance of many of the controls used to manage risk.

### Responsibilities

The Information Security Administrator has the following responsibilities:

* Ensure that security controls are in place and documented
* Manage the day to day maintenance of controls, including:
  + Access control (user account lifecycle)
  + Testing and implementing security patches
  + Vulnerability scanning
  + Software operation e.g. IDS, IPS, firewalls, DLP
  + System and network hardening
  + Remote access
  + Cryptographic key management
  + Log management
* Identify and manage information security incidents according to a process

### Authorities

The Information Security Administrator has the authority to:

* Take action to prevent an information security incident from occurring or escalating, where possible
* Maintain information security records in accordance with defined policies and procedures

## Information Asset Owner

The Information Asset Owner has primary operational responsibility for one or more information assets as defined in the *Information Asset Inventory* which indicates where personal data is stored.

### Responsibilities

The Information Asset Owner has the following responsibilities:

* Responsible for specific, named information assets
* Maintain and review security controls for allocated asset(s)
* Participate in risk assessments concerning their asset(s)
* Ensure the relevant entry in the asset inventory is kept up to date

### Authorities

The Information Asset Owner has the authority to:

* Implement controls with regard to the information assets under their control

## Information Security Auditor

The Information Security Auditor is generally responsible for checking that the information security controls used to provide GDPR compliance are effectively implemented and maintained.

### Responsibilities

The Information Security Auditor has the following responsibilities:

* Plan, establish, implement and maintain an audit programme including the frequency, methods, responsibilities, planning requirements and reporting
* Define the audit criteria and scope for each audit
* Conduct internal audits at planned intervals
* Ensure the audit process is objective and impartial
* Report the results of audits to relevant management
* Retain documented information as evidence of the audit programme and the audit results

### Authorities

The Information Security Auditor has the authority to:

* Investigate information security-related procedures and controls in order to assess their suitability and effectiveness
* Report findings to relevant management

## Data Protection Officer

The Data Protection Officer is a required appointment in line with the EU General Data Protection Regulation and has specific responsibilities for the protection of the personal data of data subjects.

### Responsibilities

The Data Protection Officer has the following responsibilities:

* Inform and advise the data controller or the processor and the employees who carry out processing of their obligations under applicable data protection law
* Monitor compliance with data protection law and with the policies of the data controller or processor in relation to the protection of personal data
* Assignment of responsibilities, awareness-raising and training of staff involved in the processing of personal data, and the related audits
* Provide advice where requested regarding data protection impact assessments and monitor their performance
* Cooperate with all relevant supervisory authorities for data protection
* Act as the contact point for supervisory authorities on issues relating to personal data processing and to consult, where appropriate, with regard to any other matter
* Act as a point of contact for use by cloud service customers regarding the processing of PII under relevant contract(s)

### Authorities

The Data Protection Officer has the authority to:

* Take decisions regarding data subject requests allowable under the relevant data protection legislation
* Represent the organization to supervisory authorities with regard to data protection issues
* Represent the organization to cloud service customers with regard to data protection issues

## Customer Information Security Administrator

[This role is primarily relevant to organizations that operate as Cloud Service Providers (CSPs).]

The Customer Information Security Administrator is a role involved in the implementation and maintenance of many of the controls used to manage risk on behalf of the cloud service customer. This role may be split between one or more employees of the cloud service customer who makes use of facilities provided as part of our cloud service offering (such as access control, user registration and data restoration) to manage the information security aspects of the service received by the customer’s users.

### Responsibilities

The Customer Information Security Administrator has the following responsibilities within the context of the cloud services provided to the customer by :

* Definition of information security requirements for cloud service
* Assess and manage risk with regard to the customer cloud environment
* Ensure that available and appropriate security controls are in place and documented within the customer cloud environment
* Manage the day to day maintenance of provided controls that relate to the customer’s specific cloud environment, including:
  + Software as a Service (SaaS)
    - Access control to cloud services, functions and data
    - User registration and deregistration
    - Multi-factor authentication
    - Management of secret authentication information (e.g. passwords)
    - Log management
    - Information labelling
    - Capacity monitoring
  + Platform as a Service (PaaS)
    - Vulnerability scanning
    - Software operation e.g. IDS, IPS, malware protection, firewalls
    - System and network hardening
    - Remote access
    - Cryptographic key management
    - Backup and recovery, including testing
    - Clock synchronization
  + Infrastructure as a Service (IaaS)
    - Installation and configuration of virtual servers
    - Testing and implementing security patches
    - Virtual network configuration
* Liaison regarding changes to the cloud environment being carried out by the cloud service provider
* Identify and manage information security events and incidents according to a process

### Authorities

The Customer Information Security Administrator has the authority to:

* Perform technical activities as defined within the scope of the cloud service agreed
* Take action to prevent an information security incident from occurring or escalating, where possible
* Maintain information security records in accordance with defined policies and procedures

# Other Roles with Information Security Responsibilities

There are a number of other internal roles within the organization which, whilst not solely dedicated to information security, have relevant responsibilities and authorities.

## Department Managers

Department Managers may be heads or supervisors of operational units within the organization.

### Responsibilities

A Department Manager has the following responsibilities:

* Review and manage employee competencies and training needs to enable them to perform their role effectively within the information security area
* Ensure that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of information security objectives

### Authorities

A Department Manager has the authority to:

* Arrange training and awareness activities for the employees under their direction, within budget constraints
* Take action to prevent an information security incident from occurring or escalating, where possible

## IT Technicians

Due to the often technical nature of information security issues, IT technicians have an important part to play in the provision and maintenance of controls.

### Responsibilities

IT Technicians generally have the following responsibilities:

* Operation of processes such as incident and change management
* Provision of technical expertise in matters of information security
* Implementation of technical controls
* System administration e.g. user creation, backups
* Security monitoring e.g. network intrusions

### Authorities

An IT Technician has the authority to:

* Take action to prevent an information security incident from occurring or escalating, where possible

## IT Users

The responsibilities of IT users are defined in a variety of organization-wide policies, and are only summarized in brief below.

### Responsibilities

An IT user has the following main responsibilities:

* Ensure they are aware of and comply with all information security policies of the organization relevant to their business role
* Report any actual or potential security breaches
* Contribute to risk assessment where required

### Authorities

An IT user has the authority to:

* Take action to prevent an information security incident from occurring or escalating, where possible