COMMUNICATION SECURITY POLICY

IT DEPARTMENT

AUDIT TEAM
ORANGE MANTRA

Contents

OM Communication security Policy

1. Introduction

1.1. Objective

Information is a key resource without which virtually all of our activities would cease. It is recognized therefore that the Company must do all it can to protect its information assets. We aim to do this in ways that are appropriate and cost-effective. This security policy aims to help enable us to fulfill our responsibilities and to ensure that a high-quality service can continue to be offered to our employees, management, and clients.

1.2. Scope

This document sets out OrangeMantra's arrangements for:

- Ensuring the protection of information in networks and its supporting information processing facilities
- Maintaining the security of information transferred both internally and with any external organization

2. Policy

2.1. Responsibilities

The Company will:

- Use all reasonable, appropriate, practical, and effective security measures to protect its business processes and information assets from inappropriate use.
- Continually examine ways in which it can improve the use of security measures to protect and enhance its business interests.
- Protect and manage its information assets in such a way as to comply with its contractual, legislative, privacy, and ethical responsibilities.

2.2. Network Security Management

2.2.1. Network controls

Our local area networks are properly managed and controlled to protect the information in systems and applications

The manager of each network is responsible for the implementation of controls to ensure the security of information, and the protection of connected services, from unauthorized access.

These controls include:

- operational responsibility for networks has been separated from computer operations unless there are good reasons for not doing so
- the establishment of responsibilities and procedures for the management of remote equipment, including equipment in user areas

- special controls to:
  - safeguard the confidentiality and integrity of data passing over public or wireless networks
  - protect the connected systems and applications
  - maintain the availability of the network services
- the monitoring and logging of security-relevant actions including, where appropriate, the use of intrusion detection systems
- close coordination between network managers to ensure the consistent application of controls

2.2.2. Security of network services

We have identified security mechanisms, service levels, and management requirements of all network services and these have been included in network services agreements, whether these services are provided in-house or outsourced.

Security features applied to network services potentially include:

- technology applied to ensure the security of network services, such as authentication, encryption, and network connection controls
- technical parameters required for secured connection with the network services in accordance with the security and network connection rules
- procedures for the network service used to restrict access to network services or applications, where necessary

The ability of the network service provider to manage agreed services securely is monitored, including through audit where appropriate

2.3. Segregation in networks

Services, information systems, users, workstations, and servers are being separated into different networks, according to defined criteria such as risk exposure and business value, and strict control of data flowing between these networks has been established.

Our basic approach to network segregation:

- networks are divided into separate logical network domains, such as internal network domains and external network domains, each protected by a defined security perimeter
- a graduated set of controls are applied in different logical network domains to further segregate the network security environments into, for example, publicly accessible systems, internal networks, and critical assets
- each such logical domain is categorized based on risk assessment, business value, and its intrinsic security requirements

- where necessary, domains are interconnected through secure gateways to control access and information flow between domains

- gateways are configured to filter traffic between these domains and to block unauthorized access in accordance with our access control policy.

2.4. Information Transfer Policies and Procedures

Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities. Such policies and procedures are important especially when information is being transferred out of or into the organization from third parties. Different but complementary controls are in place to protect information being transferred from interception, copying, modification, mis-routing and destruction and are considered holistically when identifying which controls are to be selected.

2.5. Agreements on Information Transfer

Information however being transferred, digitally or physically, agreements are addressing the secure transfer of business information between the organization and any external parties. Formal transfer policies' procedures and technical controls have been selected, implemented, operated, monitored, audited and reviewed to ensure ongoing effective security protection.

2.6. Electronic Messaging

Any information that is involved in any form of electronic messaging is appropriately protected to ensure no unauthorized access can be gained. The company has a policy which sets out which forms of electronic messaging should be used for the different types of information being transferred, e.g. Hubstaff, Thunderbird etc.

2.7. Confidentiality or Non-Disclosure Agreements

A good control describes how the requirements for confidentiality or non-disclosure agreements that reflect the organisation's needs for the protection of information must be identified, regularly reviewed and documented. As such, the company ensures that any information that needs to be protected, is done so through the use of confidentiality and non-disclosure agreements.

Agreements are specific to the company and developed with its control needs in mind following the risk analysis work. Standard agreements for confidentiality and non-disclosure that may warrant consideration here include:

- General non-disclosure and mutual non-disclosure agreements e.g. when sharing sensitive information e.g. about new business ideas.
- Customer agreements using standard terms and conditions – expressing confidentiality within the context of the use of products sold and any complementary services outlined in a related order form.
- Associate/supplier/partner agreements used for small suppliers and independent service providers who the company uses for delivery of services.
- Employment related terms.
- Privacy policies e.g. from email footers.

1. Good Practice Principles

- Using risk analysis techniques the Company will identify its security risks and their relative priorities, responding to them promptly and confidently, implementing safeguards that are appropriate, effective, culturally acceptable and practical.
- To promote better sharing and exploitation of the information, all Users will have access to appropriate internal information, including overall guidelines to the security measures employed, wherever possible.
- All Users will be accountable for their actions and all actions will be attributable to an identified individual.
- All information (including third-party information) will be protected by safeguards and handling rules appropriate to its sensitivity and criticality.
- Actual or suspected security incidents must be reported promptly.
- All Users are responsible for identifying ways in which the Security Policy might be improved.

2. Revision History

Revision	Date	Record of Changes	Approved By
1.0	1 July , 2021	Initial Policy	IT Department

3. References

Standard	Title	Description
ISO 27000:2014	Information security management systems	Overview and vocabulary
ISO 27001:2013	Information security management systems	Requirements
ISO 27002:2013	Information technology - security techniques	Code of practice for information security controls
ISO 27001:2013	Information security management systems	Clause A.14 System acquisition, development, and maintenance