Optimal Remote Security Whitepapers

OPTiM Corporation

Ver 1.0

2022/2/17

Contents

1. OPTiM Security Policy
2. System Overview
3. Server Operation
4. Data Management On Servers
5. Access Control
6. Physical Environment

OPTiM Security Policy

Basic Policy on Information Security

OPTiM Corporation (hereinafter “we/our/us”), have been developing our business with an objective to create technologies, services and business models that support customers utilizing IT. The services which we provide in our business are to make the Net as simple as breathing. Working on information security in order to provide customers with easy-to-use and secure services is one of our important missions. Thus, with an objective to achieve that mission, we decided on the Basic Policy on Information Security driving the following items, and will establish the objectives and targets of information security in accordance with the Basic Policy followed by the continuous evaluation of their accomplishments.

1. (Establishing Information Security Management System (ISMS))

With full understanding of the importance of the information assets relating to our services by all directors and staff, we establish ISMS which is organizationally and technically appropriate for protecting information assets against theft, falsification, destruction, leakage, unauthorized access etc.

2. (Information Security Management Structure)

We established the Information Security Committee as a company-wide promoting body for information security, and act aggressively to grasp the accurate status of information security throughout the company and to execute necessary countermeasures quickly.

3. (Law-observance)

We observe laws, rules, other standards and contracts applied to our information security.

4. (Protection of Information Assets)

We appropriately protect all information assets that we possess and manage by recognizing the importance from the viewpoint of confidentiality, integrity and availability, and conducting risk assessment.

5. (Enforcement of Education and Training for Information Security)

We enforce in-house education and training on information security for all directors and staff. The purpose of such training is for the staff to have recognition of the importance of information assets in order to have the Basic Policy fully understood.

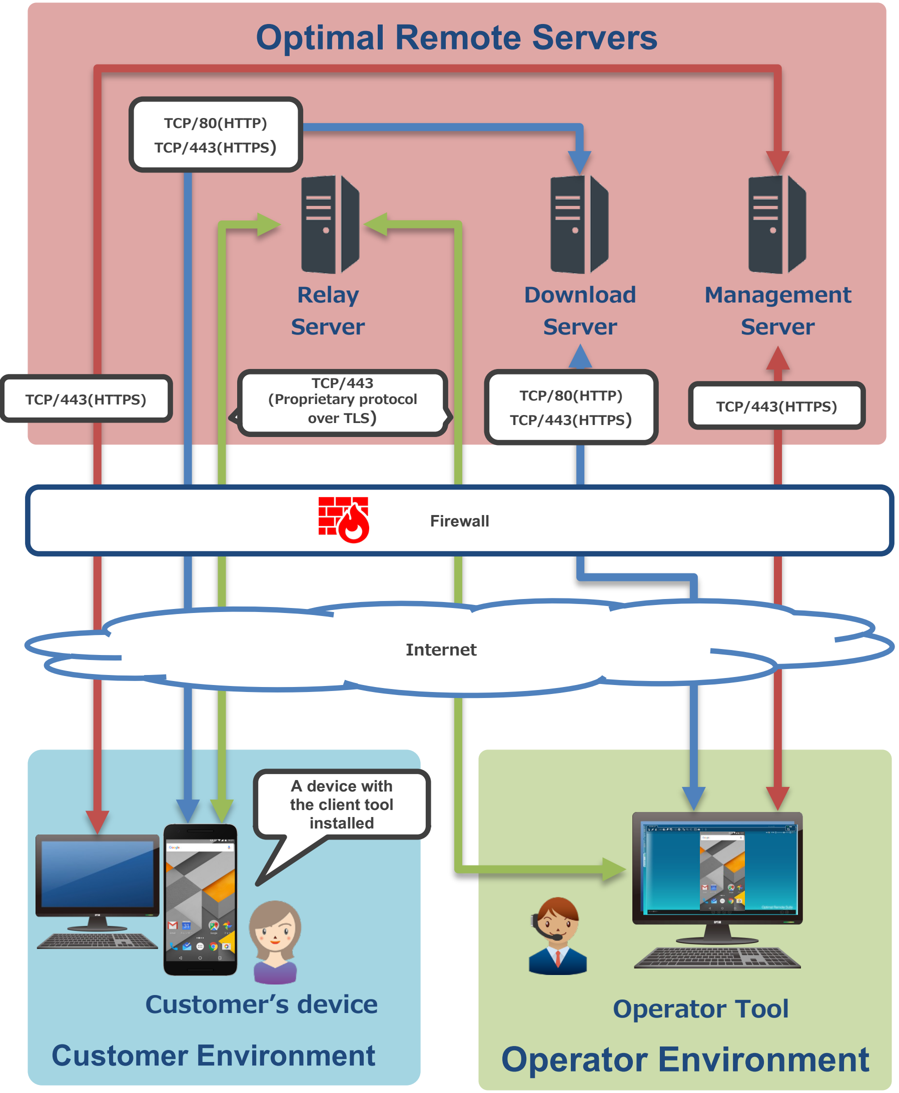
6. (Handling of Security Incident)

In case of an occurrence of an incident or signs of such on information security, we find out the cause promptly, take the best measure to keep the damage to a minimum, and strive to prevent such incident with continuous improvement.

7. (Continuous Review of ISMS)

We regularly review the Basic Policy and the relevant company regulations / management system for appropriate management and operation of information assets.

System Overview



- Optimal Remote consists of:
  - the "Operator Tool" used by the operator who provides support.
  - the "Client Tool" used by the customer who receives support.
  - servers on the internet.
- The server consists of:
  - the management server which controls connections between operators and customers.
  - the relay server which relays connections between operators and customers.
  - the download server which distributes Operator Tool and Client Tool.
- The management server, the relay server, and the download server are redundant.
- This service is connected to the internet through a firewall.

Protocol and Port

Server	Port (Protocol)	Usage
Download Server	TCP/80(HTTP) TCP/443(HTTPS)	Download the Client Tool, version up the Operator Tool
Management Server	TCP/443(HTTPS)	Operators and logs management site Login from the Operator Tool Issue a reception number The pairing of operator and customer Saving logs such as support hours
Relay Server	TCP/443 (Proprietary protocol over TLS)	Screen transfer and remote controls between operators and customers

Server Operation

- Changes to the commercial environment will be always performed after review.
- We always monitor servers and networks remotely and they can be investigated later.
- When the problem occurred, the system will make a call and send an email to the person in charge, then we fix the problem.
- We are always checking the vulnerability of OS and middleware and applying patches according to their importance and urgency.
- For security incidents, the procedure will be performed according to the defined flow.

Monitoring items (typical examples)

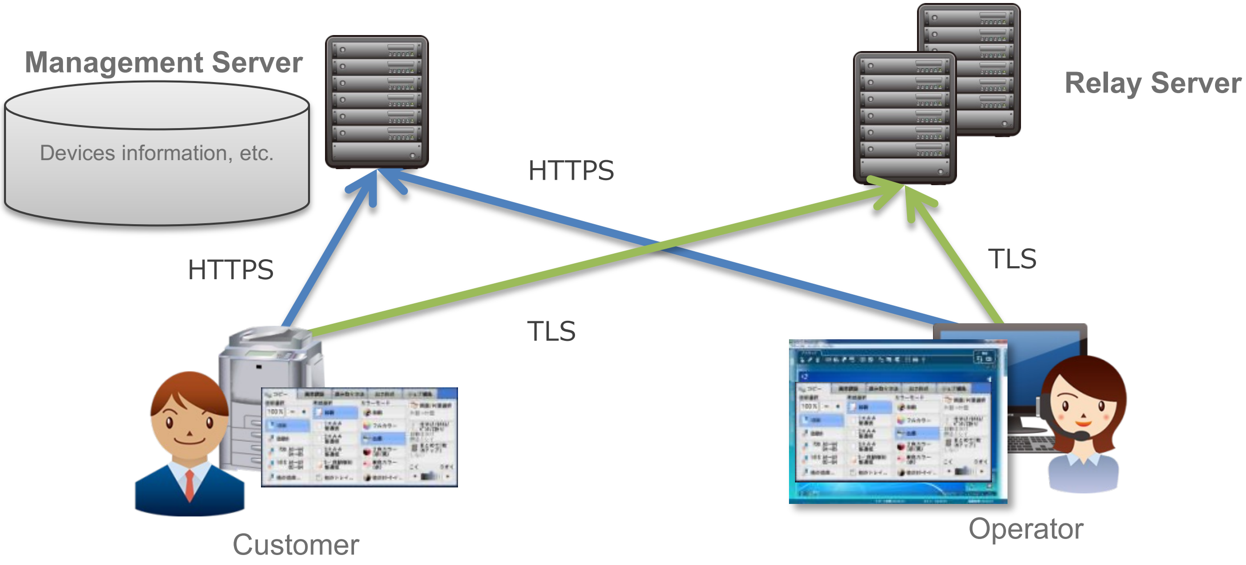
Category	Item
Service Monitoring	Service alive monitoring by HTTP/HTTPS from remote for each service.
Server Alive Monitoring	Alive monitoring for each server.
Resource Monitoring	CPU Utilization
	Memory Utilization
	Free Disk Space
	Processes
	Network Traffic

Server Operation <2>

- Availability
  - Server is available 24/7. We aim for 99.9% availability excluding planned shutdown.
  - When we stop the server for maintenance, we will notify the customers at least one week in advance.
- Software Update
  - This service uses open-source software. Whenever important security updates occur, we will update the service according to the importance.
- Recovery Procedure
  - For expected failures, the procedure will be performed according to the prepared one.
  - For unexpected failures, the procedure will be performed as soon as possible working together with developers.

Data Management On Servers

- Data, such as about customers' device information, is stored on the management server.
- Data on the shared screen will be transmitted through the relay server. No data remains on the relay server.
- All communications over the internet are encrypted by TLS.
- All data is backed up to a remote location every day, and service can be resumed using that data.



Management Server

Devices information, etc.

Relay Server

HTTPS

HTTPS

TLS

TLS

Customer

Operator

Access Control

- The Company code, the ID and the Password are required to use the Operator tool.
    - The Password must be between 8 and 20 characters with half-width alphanumeric characters or half-width symbols.
    - The Password will be saved after hashing.
    - There is a function to lock accounts after a certain number of incorrect passwords have been entered.
- The Company code are managed by OPTiM.
- The Administrator account can be issued by the company, and the Administrator account can manage operators.
- Server management in OPTiM.
    - Server management and Data management need dedicated ID.
    - The ID is managed by ID management base.
    - Management of commercial environment is performed by limited people.
    - Accounts that are no longer needed by retirement or transfer will be stopped immediately.

Physical Environment

- Commercial environment are built on internet data center or IaaS provided on internet data center.
- Internet data center are installed Security Cameras and Security Gates and are built in building can withstand earthquakes.
- All systems are installed behind the firewall.

Data center specification

	Japan	Europe	North America
Certification	ISO27001 or ISAE3402/SSAE16	ISO27001:2005 and ISO9001	SSAE16 SOC-1 Type II
Location	Japan domestic	Amsterdam	San Francisco
Building	Dedicated building.	non-disclosure	non-disclosure
Earthquake resistance	Designed to withstand a seismic intensity of 7.	non-disclosure	non-disclosure
Uninterruptible Power Supply	installed	installed	installed
Power supply route	Extra High Voltage, Dual feed	non-disclosure	non-disclosure
Emergency private power generation facility	installed	installed	installed
Fire extinguishing equipment	Fire extinguishing equipment and automatic fire extinguishing equipment	VESDA	non-disclosure
Lightning protection	Countermeasures against direct lightning strikes: installed Countermeasures against induced lightning strikes: installed	non-disclosure	non-disclosure
Access Control System	Access records period: 7 years Security camera storage period: 3 months Personal authentication system: installed	Security camera: installed Personal authentication system: installed	Security camera storage period: 90 days

OPTiM

www.optim.co.jp

About security of Optimal Remote