

CONFIDENTIAL

# INFORMATIONS ABOUT SECURITY FEATURES AND CONCEPTS USED IN AGILE.IT INFRASTRUCTURE MANAGEMENT CONTEXT



## Contents

|   |                                     |
|---|-------------------------------------|
| Document statement .....                  | 2                                   |
| Purpose.....                              | 2                                   |
| Recipient.....                            | 2                                   |
| Confidentiality .....                     | 2                                   |
| Revision .....                            | 2                                   |
| Schematic Overview .....                  | 3                                   |
| Platforms presentation.....               | 4                                   |
| Connect .....                             | 4                                   |
| Remote session .....                      | 4                                   |
| Dimension.....                            | 4                                   |
| COGNiKA.....                              | <b>Error! Bookmark not defined.</b> |
| Office 365 .....                          | 4                                   |
| Remote Maintenance.....                   | 4                                   |
| General Concept.....                      | 5                                   |
| Distributed design .....                  | 5                                   |
| User credentials.....                     | 6                                   |
| Auditing .....                            | 6                                   |
| Roles based Design.....                   | 7                                   |
| Security baseline .....                   | 7                                   |
| Platforms details.....                    | 8                                   |
| Connect .....                             | 8                                   |
| Architecture.....                         | 9                                   |
| Remote Session .....                      | 10                                  |
| COGNiKA.....                              | <b>Error! Bookmark not defined.</b> |
| Dimension.....                            | 12                                  |
| Office 365 .....                          | 14                                  |
| User environment.....                     | 15                                  |
| Backup & recovery .....                   | 16                                  |
| Deprecation of VPN IPsec technics .....   | 17                                  |
| Data breaches.....                        | 19                                  |
| Identification .....                      | 19                                  |
| Reporting.....                            | 19                                  |
| Requests on sensitive information's. .... | 20                                  |
| ANNEXES.....                              | 21                                  |

## Document statement

### Purpose.

This document is used to provide an overview of security technics used in NETiKA IT Services customers IT operational management to secure sensitive data and infrastructures.

### Recipient

This document is transmitted to: XXXXXXXXXXXXXXXXXXXXX

### Confidentiality

Information contained are only intended for the person identified in this form as recipient

NETiKA IT Services and the Customer are bound by an obligation of confidentiality relating this document and all confidential information they receive from each other. This confidentiality obligation also applies to their Employees and to any Sub-processor and their employees.

This confidentiality obligation takes effect upon communication of this Document, remains valid during the entire duration of the collaboration and after the termination of the collaboration.

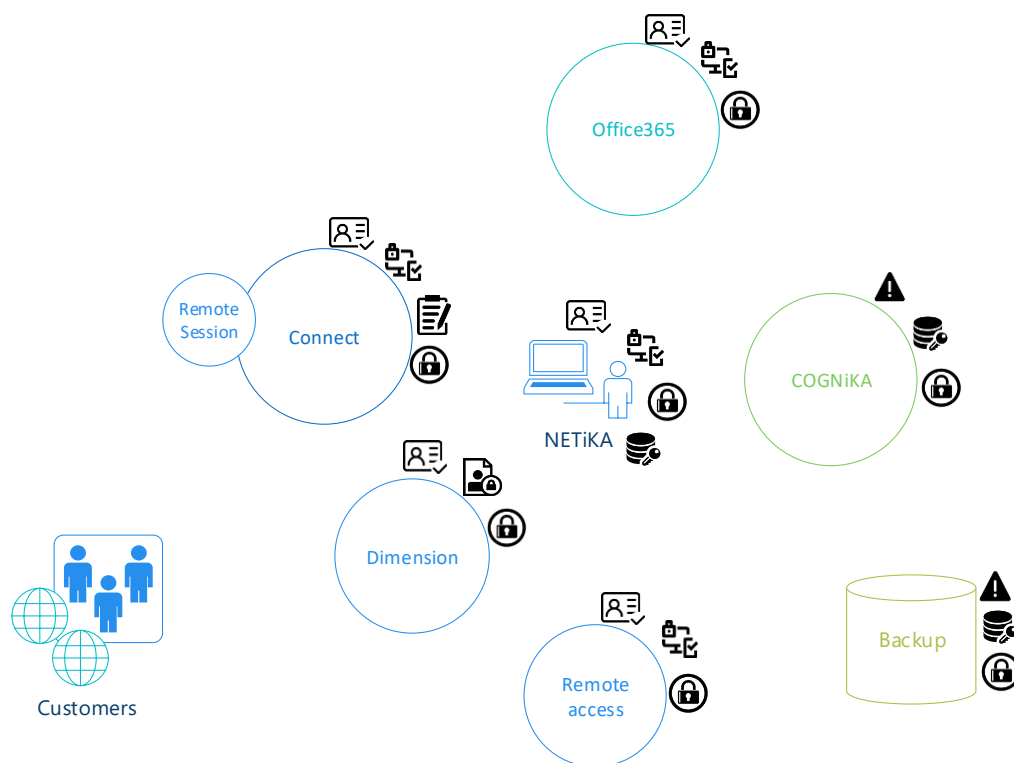
### Revision








Last update on 24-10-2018

## Schematic Overview

The following schema help quickly identify NETiKA IT Services services/applications/platforms in regard on security considerations.

Note: Details related to each platform will be presented in the Service details sections



|   |                                |
|---|--------------------------------|
|  | Nominative Authentication      |
|  | Two Form-Factor Authentication |
|  | Privacy / Personal data        |
|  | Logging & audit trail          |
|  | Traffic Encryption             |
|  | Specific Records Encryption    |
|  | Restricted zone                |

## Platforms summary

### Connect

Connect is NETiKA IT Services Remote Monitoring & Management Platform.

As a centralized operational platform to manage Customers Infrastructure, it provides us facilities including: Remote monitoring, Automation, Inventory, Patch management, Reporting.

### Remote session

Remote Session is a component of the Connect platform used to take control remotely over servers and workstations to provide technical support, troubleshooting, operations and maintenance.

### Dimension

Dimension is used for Firewall security services logging. It provides data visibility and reporting tools that identify insight, accelerating the ability to set meaningful security policies for Customers and troubleshoot performance, application and security issues by using advanced logging facility.

### COGNiKA

COGNiKA is a documentation platform specially developed to store sensitive IT oriented objects as password, devices, certificates.

### Office 365

Office 365 is a suite of applications used to provide office applications as email, CRM, digital documents library;

### Remote Maintenance

Remote Maintenance is a set of technics use to establish secure connection between:

- Customers and NETiKA IT Services Office's or Datacentre's.
- NETiKA IT Services employee and NETiKA IT Services Office's or Datacentre's

Previously, this platform was used in a bidirectional way (customers to NETiKA IT Services) to provide secure connection and serve as a base for Remote Management & eMonitoring services.

Note: This usage has been deprecated (refer to "Deprecation of VPN technics" section)

# General Concept

## Distributed design

Services are distributed across different platforms and compartments.

As an example, the operation platform doesn't store any operational passwords, passwords are stored in a specific database.

Benefits of this approach:

- Services are not hosted in the same compartment.
- Data are not stored in a same unique database.
- Facility to close a compartment in case of data breach.
- Interactions between platforms are restricted to trusted tiers.
- Limit data breach spreading.
- Enforce each compartment with the most appropriate security approach.

Compartments can be a Network area as DMZ, an isolated datacentre/ hosting or a hosted service.

Connections between compartments are ruled by security equipment's applying a set of traditional security technics as: Authentication, Intrusion Prevention System, Encryption, Antivirus, Reputation-Based Threat Prevention, Threat Detection, URL/IP Filtering .

Note: For security reason, description of these technics is out of the scope of this document but can be specifically answered on demand.



## User credentials

Each employee of NETiKA IT Services IT services are titular of a unique personal and nominative credential. (ex: John Collins)

Use of generic account are not allowed to manage customers via operational platforms.

To maintain a single centralized management across the distributed platform design, user accounts are centralized in an [Active directory](#) and security options are enforced by a set of policies (refer to annexes for samples)

However, depending of the risk level and exposed surface of platforms, authentications are enforced by a Multifactor Authentication process to mitigate impact of stolen credentials.



NETiKA IT Services use Multi Form Factor technologies [Azure Authenticator](#) and [AuthPoint](#) depending on the level of complexity required.





























































## Auditing

Multi-Form factor authentication process are real time audited , provide us ability to be notified in case of abnormal authentication process or authentication incidents.

## Roles based Design

All platforms integrate a role-based model that give the ability to clearly design roles required by the operational processes.

The role-based model is also used to provide strict access for customers to facilitate customer involvement.






|                          | Name   | Users                       | Permissions   |
|--------------------------|--|-----------------------------|---|
| <input type="checkbox"/> | Non Technical Users - Customers - NETIKA Standard    | Non Technical Users         | (Details)      |
| <input type="checkbox"/> | Technical Advanced Rights - ITS - NETIKA Standard    | Technical Advanced Rights   | (Details)      |
| <input type="checkbox"/> | Ecran Controle - NETIKA Standard                     | Ecran Controle              | (Details)      |
| <input type="checkbox"/> | Technical Basic Rights - Customers - NETIKA Standard | Technical Basic Rights      | (Details)      |
| <input type="checkbox"/> | Non Technical Users - ITS - NETIKA Standard          | Non Technical Users         | (Details)      |
| <input type="checkbox"/> | Technical Basic Rights - ITS - NETIKA Standard       | Technical Basic Rights      | (Details)      |
| <input type="checkbox"/> | Default Technician Role                              | Default Technician Role     |                |
| <input type="checkbox"/> | Default Remote Control Role                          | Default Remote Control Role |                |
| <input type="checkbox"/> | Default Dashboard Role                               | Default Dashboard Role      |                |
| <input type="checkbox"/> | Default Administrator Role                           | Default Administrator Role  |                |
| <input type="checkbox"/> | Task Force - NETIKA Standard                         | Task Force                  | (Details)      |
| <input type="checkbox"/> | admin(at)agile-it.be                                 | admin(at)agile-it.be        | (Details)      |

Sample of roles extract

## Security baseline

The following table present the security baseline used by default.

if a service benefit of a supersedes or enforced technics, there are described in the detail's sections.







|   |   |
|---|---|
|  | Kerberos AES 256  |
|  | Two-Form factor authentication enforcement on sensitive services and data.            |
|  | Logging & audit trail active  |
|  | Traffic Encryption: SSL certificate SHA256 G2 RSA 4096 ( <a href="#">GlobalSign</a> ) |
|  | Roles are designed to restrict usage.   |



## Platforms details

This section provides more details on technics used to mitigate inherent risk on the platforms or handle a specifics security area.

### Connect

|  |   |
|--|---|
|   | Nominative Authentication: Yes  |
|   | Two Form-Factor Authentication: Yes<br>*Per customer additional Authentication: Yes |
|   | No personal/privacy/enterprise files are recorded or processed by the system.       |
|   | All operations and access are logged and digitally recorded in the audit trail logs |
|   | Traffic Encryption: Yes   |
|  | Specific Records Encryption: Yes  |

## Architecture

As a direct result of the Connect architecture, there is no public IP address, port forwarding, or incoming VPN's required to connect the service or establish a remote session.

The outbound communications from customer devices to the Connect service are based on SOAP and XMPP and are transmitted using the HTTPS protocol.






After the outbound session is established, the devices receive a session ID that is used to identify that session and it persists until the session is closed. The device will open a second (asynchronous) signalling channel leveraging the XMPP protocol. In cases where the XMPP session is terminated abnormally (for example, by a firewall cleaning open sessions), the device will re-create the session automatically. Connect leverages the XMPP based communications for control purposes only, not for the transmission of monitored data.

By default, the devices and XMPP-based communications use HTTPS with the data encrypted using TLS and the strongest cipher suite supported by the customer devices version.

| AUDIT TRAIL  |                               |                |                        |                |                       |  |
|--|-------------------------------|----------------|------------------------|----------------|-----------------------|--|
| CREATE TICKET  |                               | UPDATE TICKET  |                        |                |                       |  |
| Enter search criteria                                    |                               | SEARCH         | RESET FILTER           |                |                       |  |
| <input type="checkbox"/> Date                            | <input type="checkbox"/> User | Category       | Feature                | Action         | Status                | Details  |
| <input type="checkbox"/> Thu, Jun 07, 2018 01:58 PM CEST |                               | Monitoring     | Monitoring             | Disable        | ✓                     | • hyper-v 2012 Guest Status - 113-DIMENSION-4<br>Start Time: 2018-01-26 12:02:50<br>End Time: 2018-01-26 12:07:10<br>Duration: 0 Hours 4 Minutes 19 Seconds<br>Session Logs: <a href="#">Click here</a>                    |
| <input type="checkbox"/> Fri, Jan 26, 2018 12:02 PM CET  |                               | Remote Control | Take Control           | Remote Session | ✓                     | Start Time: 2017-09-29 16:56:56<br>End Time: 2017-09-29 17:01:24<br>Duration: 0 Hours 4 Minutes 28 Seconds<br>Session Logs: <a href="#">Click here</a>   |
| <input type="checkbox"/> Fri, Sep 29, 2017 04:56 PM CEST |                               | Remote Control | Take Control           | Remote Session | ✓                     | New Startup Type: Automatic<br>• Print Spooler: Succeeded<br>Start Time: 2017-09-29 16:54:07<br>End Time: 2017-09-29 17:54:35  |
| <input type="checkbox"/> Fri, Sep 29, 2017 04:55 PM CEST |                               | Direct Support | Service Management     | Startup Type   | ✓                     | • Print Spooler: Succeeded   |
| <input type="checkbox"/> Fri, Sep 29, 2017 04:54 PM CEST |                               | Direct Support | Command Prompt         | Session        | ✓                     | Start Time: 2017-09-29 16:51:24<br>End Time: 2017-09-29 17:01:26<br>Duration: 0 Hours 10 Minutes 2 Seconds<br>Session Logs: <a href="#">Click here</a>   |
| <input type="checkbox"/> Fri, Sep 29, 2017 04:53 PM CEST |                               | Direct Support | Service Management     | Start          | ✓                     | Start Time: 2017-09-29 16:49:55<br>End Time: 2017-09-29 16:51:17<br>Duration: 0 Hours 1 Minutes 21 Seconds<br>Session Logs: <a href="#">Click here</a>   |
| <input type="checkbox"/> Fri, Sep 29, 2017 04:51 PM CEST |                               | Remote Control | Take Control           | Remote Session | ✓                     | Start Time: 2017-09-29 10:37:16<br>End Time: 2017-09-29 10:37:19<br>Start Time: 2017-09-28 16:13:20<br>End Time: 2017-09-28 16:30:27<br>Duration: 0 Hours 17 Minutes 6 Seconds<br>Session Logs: <a href="#">Click here</a> |
| <input type="checkbox"/> Fri, Sep 29, 2017 04:49 PM CEST |                               | Remote Control | Take Control           | Remote Session | ✓                     |  |
| <input type="checkbox"/> Fri, Sep 29, 2017 10:37 AM CEST |                               | Direct Support | Command Prompt         | Session        | ✓                     |  |
| <input type="checkbox"/> Thu, Sep 28, 2017 04:13 PM CEST |                               | Remote Control | Take Control           | Remote Session | ✓                     |  |
| REFRESH NOW  |                               | ON             | Refresh in: 10 minutes |                | Selected: 0 Total: 13 |  |

Example of logging and audit trail view

## Remote Session

|   |   |
|---|---|
|  | Nominative Authentication: Yes  |
|  | Two Form-Factor Authentication: Yes<br>Per customer additional Authentication: Yes                                    |
|  | Specific features to address privacy issue related to remote session over User devices*                               |
|  | All major features, including remote control, file transfer and chat conversations are logged in the Session details. |
|  | Traffic Encryption: Yes<br>AES 256  |

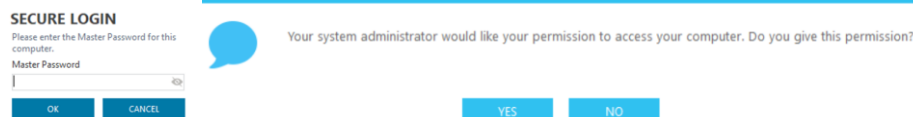
Note: As Remote Session is a component of Connect, it benefits on the same connectivity model as described in previous chapter.

Remote sessions are sheltered by a proprietary communication protocol with guaranteed global security by encryption standard AES using a 256-bit cipher (both when establishing or for the duration of the session). The key exchange is protected by an SSL based in AESCBC with TLS v1.1.







All commands, including keyboard and mouse strokes, file transfers and clipboard information are digitally signed. All encryption is based on an end-to-end negotiation that does not intercept transferred information or decode the information in the gateway. Encryption keys are randomly generated for each session.

\*As an additional security measure, the authentication method is enforced using a per customer Master Password and a pre-authorization confirmation by the users to launch the session to protect privacy and unexpected remote session on users' devices (ex: laptops, desktops and mobile devices)

The use of Master Password doesn't bypass the Customer Devices Credentials that are still needed after the pre-authentication. As a result, the security chain policy implemented at customer level is not broken at any time.



Per customer master -password or Pre-authorization in user session handover scenario

|   |  |
|---|--|
|  | Nominative Authentication: HMAC-SHA256-PBKDF2                                |
|  | Two Form-Factor Authentication: In progress                                  |
|  | All operations on sensitive data are logged                                  |
|  | Traffic Encryption: Yes  |
|  | Specific Records Encryption:<br>Sensitive Data encryption algorithm: AES-256 |
|  | Restricted zone:<br>The platform is isolated in a restricted area.           |

Changes and visualizations of sensitive information's are limited to authorized roles, are logged, and each user accessing it sees the log of previous accesses (date, user, read action or write).

To secure sensitive data, print report generated as PDF from COGNiKA doesn't include any credentials.

| Confirmation   |      |         |  |
|--|------|---------|--|
| Are you sure you need to view this confidential information (access will be logged)? |      |         |  |
| Date   | User | Actions |  |
| 12/10/2018 10:02   |      | View    |  |
| 11/10/2018 15:35   |      | View    |  |
| 08/10/2018 15:36   |      | View    |  |
| 08/10/2018 14:30   |      | View    |  |
| 02/10/2018 15:23   |      | View    |  |
| 02/10/2018 10:38   |      | View    |  |
| 01/10/2018 10:12   |      | View    |  |
| 01/10/2018 09:47   |      | View    |  |
| 28/09/2018 11:43   |      | View    |  |

Example of sensitive data access:

#### Account security: Skype







##### General

| General   |   |
|-----------|---|
| Name*     | Skype   |
| Tech note | Compte Skype Generic  |
| Tiny url  | <a href="https://cognika.netika.com/cognika2/View.ashx?ref=CognikaAccountSecurity/60233">https://cognika.netika.com/cognika2/View.ashx?ref=CognikaAccountSecurity/60233</a> |

| Account/Security |             |                           |          |               |             |
|------------------|-------------|---------------------------|----------|---------------|-------------|
| Name             | Description | Login                     | Password | Secret answer | License key |
| Skype account    |             | informagiciens@netika.com | *****    |               |             |

Example of pdf/print report

## Dimension

|   |  |
|---|--|
|  | Nominative Authentication: Yes   |
|  | System record potential personal data<br>Data are retained for a fixed period of 30 days<br>Deletion of data occur every 30 days |
|  | Logging & audit trail: Yes   |
|  | Traffic Encryption: Yes  |
|  | Specific Records Encryption: Yes<br>Logs are fully encrypted   |
|  | Restricted zone  |

Dimension are used to store insight and logging coming from Customers security devices.  
The goal of this platform is to provide visibly for advanced debug technics.

Depending on the customer firewall's setup, the platform can record potential user personal data as visited websites, traffic habits, unprotected credentials, etc...

To protect these personal data, records are anonymised by default and enforced by a set of rules.

When users log in to Dimension, log messages and detail reports are not available. Instead, users only see a restricted view of the pages.

Anonymized placeholder text uses a standard pattern for each data type, is randomly generated, and is different for each user session. Placeholder text includes a randomly generated sequence of letters and numbers, and begins with these prefixes: USER, DEVICE, HOST, IP-ADDRESS.

When Anonymized Mode is enabled and accessing the log is needed to process a technical relevant request, a user with the Anonymization Officer role can log in as a secondary user for a current user session and temporarily disable Anonymized Mode for only that session. When Anonymized Mode is temporarily disabled, the current user can see the data that was anonymized. When the current user logs out and logs in again, Anonymized Mode is enabled again.

This Anonymization Officer role can only be held by a NETiKA IT Services employee.

Customers authorized to access the platform are not allowed to claim Anonymised Officer role.

In case of customers request to access un-anonymised reports or information's , this require a specific form application. (Refer to the "Sensitive Information Request" section)

Top Clients

View All

| NAME   | BYTES | HITS   |
|--|-------|--------|
| IP-ADDRESS:2A42-36E1-272E-3974-476F-A7D6-E3B2-97B8-8066-1D99-B6... | 6 GB  | 85,798 |
| IP-ADDRESS:8A39-9E53-5DF6-AE60-B87B-D1EE-ED62-4751-5E53-FA20-3B... | 4 GB  | 77     |
| IP-ADDRESS:371C-311C-3CAE-5C1D-B12F-852F-F3AD-19A4-ACD3-1981-1...  | 3 GB  | 7,188  |
| IP-ADDRESS:6F85-0C7D-0069-2990-4F41-D3DD-D7AB-16F7-A3B2-BFF0-8...  | 2 GB  | 9,248  |
| IP-ADDRESS:7813-B979-077A-5B21-B361-ED0A-F5F3-DB8C-9E3B-8CC2-1...  | 2 GB  | 5,367  |
| IP-ADDRESS:906A-8A0A-1C1F-372F-BD2F-7CBC-A39A-7041-AF71-730D-E...  | 2 GB  | 4,507  |
| IP-ADDRESS:A898-9DD9-FE3A-03A2-9947-0664-EE0C-1B90-086A-8C44-15... | 2 GB  | 29,246 |
| IP-ADDRESS:7C7B-4854-271E-AEA9-1C40-3E4C-4772-2360-3BFF-F219-60... | 1 GB  | 10,383 |
| IP-ADDRESS:5D36-7924-E01E-55D7-94FA-2274-1109-96CB-FF1D-9F20-2A... | 1 GB  | 29,580 |
| IP-ADDRESS:ACC5-21CE-F91E-DFE6-F4A4-9C43-CA46-B709-1C52-9095-D6... | 1 GB  | 8,492  |

Sample of Anonymized data view

Disable Anonymized Mode

To temporarily disable Anonymized Mode for only this user, specify your Anonymization Officer credentials. The user will then be allowed to see the anonymized data for only the current session. When the user logs out and logs, Anonymized Mode will be enabled.

User Name

User Name






Passphrase

Passphrase

CANCEL

OK

Approbation to disable anonymization

|   |  |
|---|--|
|  | Nominative Authentication: Yes   |
|  | Two Form-Factor Authentication: Yes  |
|  | Use of Personal Certificate to trust user Identity   |
|  | Logging & audit trail: Yes   |
|  | Traffic Encryption: Yes<br>Email Traffic are encrypted using TLS if supported by customer. |

Personal Digital Certificate is a Digital ID issued to an entity that helps to prove that entity's identity. The Digital ID binds an individual's verified identity (typically including the name, company name, and email address of the Digital ID owner) to a unique cryptographic credential.

Personal Certificates allow NETiKA IT Services individuals to represent their digital identities using digital signatures in many applications, from secure email to two factor authentications, and document signing.

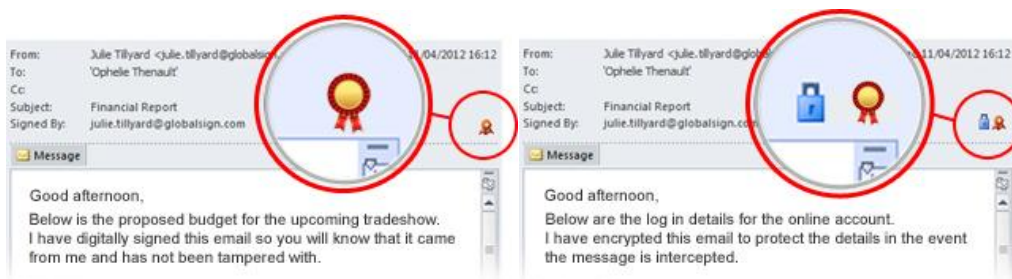
As a result, customers can easily make sure of the sender or the source of the information

Certificates use S/MIME technology to allow users to digitally sign and encrypt email.

**Digitally signing an email** proves authorship and prevents tampering, assuring the email recipient that the email came from NETiKA IT Services, not an imposter, and that the content of the email has not been altered in transit.

**Encrypting email** ensures message privacy and keeps sensitive information from falling into the wrong hands. This technic is only available if digital certificate is supported by both party







Personal Certificates are provided by trusted certificate provider [GlobalSign](https://www.globalsign.com/)



## User environment

NETiKA IT Services employee Workstations or Laptop use a set of security features enforced by policies.

All workstations or laptops are protected by enforced firewall and Antivirus engine (Bitdefender)





|   |  |
|---|--|
|  | Nominative Authentication: Yes   |
|  | Two Form-Factor Authentication: Yes  |
|  | Use of Personal Certificate to prove user Identity in supported applications |
|  | Logging & audit trail: Yes   |
|  | Traffic Encryption:<br>SHA256 AES Open SSL connection                        |
|  | Hard drive encrypted via <a href="#">Bitlocker</a>                           |

Note: Sample of Security applied policy extract are available in annexes



## Backup & recovery

Backup and recovery features permit us to quickly recover services and data in case of data lost or system failure.

|   |  |
|---|--|
|  | Logging & audit trail: Yes   |
|  | Traffic Encryption:<br>256-bit Advanced Encryption Standard (AES)            |
|  | Storage Encryption:<br>256-bit AES with a 256-bit key length in the CBC-mode |
|  | Restricted zone:<br>Backup are stored in dedicated zone                      |

All operational platforms (except Office365) are backup two times per day and subject to regular recovery plan testing.






## Deprecation of VPN IPsec technics

VPN IPsec technics are used to establish bilateral secure connections between customers and NETiKA IT Services Office's / Datacentres. The main purpose of this technics is to permit secure use of managed remote services as Remote Maintenance and eMonitoring.

It's also used to provide secure access from customer to restricted NETiKA IT Services Platform.

These technics has been deprecated since deployment of lasted agile.IT version and are now optional.

For practical reasons, IPsec VPN's still in use for some clients but only address specifics need and his subject to future roll-out.

|   |  |
|---|--|
|    | Nominative Authentication: Yes   |
|    | Two Form-Factor Authentication: In progress  |
|    | Logging & audit trail: Yes   |
|    | Tunnel Authentication:<br>SHA1-AES 256 DF5<br>(depending on customers compatibility backwards) |
|  | Traffic Encryption:<br>ESP-AES-SHA1<br>(depending on customers compatibility backwards)        |

### Outgoing traffic rules applied

| Source (NETiKA IT Services)                | Ports Allowed | Destination (Customer)  |
|--|---------------|---|
| Authorized NETiKA IT Services employees    | 3389 TCP      | Restricted list of devices allowed by the customer.<br>Enforced on Customer VPN devices |
| Enforced on NETiKA IT Services VPN devices | 80 TCP        |   |
|  | 443 TCP       |   |
|  | 4040 TCP      |   |
|  | 8080 TCP      |   |
|  | 4130 TCP      |   |
|  | 5000 TCP      |   |
|  | 5001TCP       |   |
|  | 22 TCP        |   |
|  | 8443 TCP      |   |
|  | 23 TCP        |   |
|  | 23 UDP        |   |
|  | 161 UDP       |   |
|  | 4105 TCP      |   |
|  | 4117 TCP      |   |

### Incoming traffic rule applied

| Source (Customer)   | Ports Allowed | Destination (NETiKA IT Services)  |
|---|---------------|---|
| Restricted list of computer/user<br>Enforced on NETiKA IT Services<br>VPN devices | 443    TCP    | Restricted list of services.<br>Enforced on NETiKA IT Services<br>VPN devices |

# Data breaches

## Definition

A Data breach is a breach of the security of Data which inadvertently or unlawfully leads to the destruction, loss, modification or unauthorized disclosure of or unauthorized access to data transmitted, stored or otherwise processed.

## Identification

The Identification of Data Breach rely on technical and human detection of abnormal processes or events traced back by monitoring tools, events engine or regular audit.

When a Data Breach is detected, it will be reported to both our Emergency Technical Team and our GDPR Officer.

The purposes of this mechanism are:

- Take appropriate counter-measures without delays to mitigate the Data Breach impact.
- Assure that the event is processed and ruled as defined in the reporting section.

## Reporting

If NETiKA IT Services notices a Data Breach <sup>(\*)</sup>, we will notify the impacted customers without undue delay, and at the latest within 48 hours after the Data Breach has been noticed. The notification will be accompanied by any useful documentation to permit the customer(s), if necessary, to notify the Data Breach to the GDPR Supervisory Authority and/or the Data Subjects. The notification shall at least provide or describe the following:

- The nature of the Data Breach in relation to the Customer Data;
- The categories of Data concerned;
- The consequences that are likely to happen because of the Data Breach regarding the Data;
- The measures proposed or taken by the Customer to address the Data Breach, including, where appropriate, the measures to mitigate any adverse effects.

It is up to the Customer to assess whether or not he will inform the Supervisory Authority and/or the its users about the Data Breach.

## Requests on sensitive information's.

Requests involving sensitive information's are processed through specifics application forms.

These application forms can be applied by NETiKA IT Services employees to revoke the request and ask for Customer Representative agreement prior processing it.

Examples of cases requiring a special application form:

- Reset or change of a user password.
- Reset or change of administrator/systems credentials.
- Transmission of confidential information.
- Request to change rights on personal storage: mailboxes, file storage, identities.
- Request to report individuals' activities.
- **All requests NETiKA IT Services deem necessary the application of this rule.**

Note: Sample of this application form available in annexe.

## ANNEXES

### *Sample of Sensitive Information Request Form*

Hello,

We have received your request below regarding the *access of a user's mailbox*.

The Penal Code, the law of June 13, 2005, the General Regulation on the Protection of Personal Data (RGPD), the Collective Labor Agreement n ° 81 (CCT81) ... very strictly regulate the access to the mailbox of a worker. Before completing the requested transaction, we would like to remind you of the duties and procedures that any employer must follow to access an employee's mailbox. You will find below a summary of the legal rules and case-law concerning the control of workers and / or the collection of personal data.

We ask you to ensure compliance with these rules and in default of respecting them, to confirm by response to this email that you agree to cover the full costs incurred (administrative costs, justice, experts, advice and others ...) in the event of a lawsuit or complaint against NETIKA IT SERVICES for the violation of your worker's privacy. We assure you of course the confidentiality of your request and any actions taken.

Best regards

XXX

The right to respect a worker's life privacy is a principle of law which is enshrined in various regulations and in Article 22 of the Belgian Constitution. This principle of law establishes a prohibition in principle of employer control over the use of electronic means of communication by its employees.

1. Article 314bis of the Penal Code prohibits any recording of private communications or telecommunications by a person who does not participate, unless the consent of all participants in the communication (This article is only applicable at the moment It is not applicable when e-mails can be found via Internet history and copying a hard drive (Brussels Court of Work, 4 August 2016).

2. The law of 13 June 2005 on electronic communications introduces a similar provision in Article 124. This article prohibits anyone from reading the existence of information of any kind (private communication and professional communication). ) transmitted by electronic communication and which is not intended for him personally, unless authorized by all persons directly or indirectly concerned.

However, there are exceptions to this principle of prohibition of electronic communications in the following cases:

- if the employer obtains the consent of all the participants in the communication. Which is very theoretical, because it will be difficult for the employer to obtain the consent of the participants to the communication which are external to his company ...

- if a specific law authorizes this acquaintance.

With regard to this second exception, some of the case-law considers that the Employment Contracts Act constitutes a sufficient legal basis for this purpose because it contains provisions relating to the authority of the employer (Articles 2, 3, 4 and 5) and the duty of mutual respect (Articles 16 and 17). This position, however, is criticized by the doctrine, which points to the vague nature of these two provisions so that they can constitute a valid exception to Article 124 of the Act of 13 June 2005.

3. The Privacy Law of December 8, 1992 and soon, May 25, 2018, the General Regulations on the Protection of Personal Data (RGPD) are aimed at the protection of individuals with respect to the processing of their personal data. Is a personal data, a login, an email address, ... Under these two laws, control information generated by the electronic communication tools used by the worker in the context of the employment relationship generally requires a treatment of personal data. Such processing of personal data is only permitted subject to compliance with the following principles:

- the principle of finality: the treatment must take place for specified purposes, expressly described and justified;
- the principle of proportionality: the processed data must be sufficient, useful and not excessive, in relation to the objectives for which they are obtained and for which they are then processed;
- the principle of transparency: certain information must be provided to workers, particularly with regard to the purpose of the processing.

Moreover, such treatment must be the subject of a declaration of treatment made to the Commission Privacy, before processing begins and soon, under the RGPD, keep the evidence in a data processing registry before processing the treatment, the controller has applied the principles "by design", by default, and the bare necessities.

4. The Collective Labor Agreement n ° 81 (CCT81) ensures the respect of the worker's private life when a collection of data of electronic communication in network is established by the employer to make the control and resumes the principles purpose, proportionality and transparency. CTC 81 does not deal with the question of

whether the contents of the files created by the worker and stored in a company computer, or the content of the e-mails sent and / or received by the worker by means of the company. However, some judges still apply the 3 principles of CTC 81. It is therefore strongly recommended that the employer respect the 3 principles and the procedure described in CTC 81 when he wishes to control the use electronic tools made available to its workers. The employer must, before any installation of any control system, first make a collective information of the workers, via the works council (CE), or in the absence of the committee for prevention and protection at work (CPPT), or failing that, the trade union delegation, or failing that, directly to the workers. When installing the networked electronic communication data control system, the employer must then proceed to individual information via general instructions, or references in the work regulations, or in the individual employment contract, or by instructions for use provided with each use of the tool. The individualisation of networked electronic communication data must also respect the principles of finality, proportionality and transparency.

For purposes such as:

- The prevention of unlawful or defamatory facts, acts contrary to morality or likely to affect the dignity of others;
- The protection of the economic, commercial and financial interests of the company to which is attached a character of confidentiality as well as the fight against the contrary practices;
- The security and / or technical functioning of the company's networked computer systems, including the control of related costs, as well as the physical protection of the company's facilities; the employer can carry out an individualisation directly, as soon as he notices an anomaly. On the other hand, if the control pursues as an aim the respect in good faith of the principles and rules of use of the technologies fixed in the company, the individualisation must be indirect, that is to say, preceded by a preliminary phase of information. In this case, it is necessary to inform the worker of the existence of the anomaly and to inform him / her of an individualisation of the electronic communication data when a new anomaly of the same nature is detected. In addition, the employer must also invite the worker concerned to an interview, to enable him to inform the employer of his objections to the decision or the assessment envisaged and to explain himself the use made by him of the means of electronic communication made available to him.

What are the penalties for violating the right to privacy?

The worker can claim compensation for damages. This repair turns out to be very often of the "moral damage" type. In addition, criminal penalties are also provided for the employer who violates the provisions of CTC No. 81.

#### Conclusion

It is noted that in all cases, the control of email and instant messaging of workers must always be done in accordance with the principles of legality, finality and proportionality.

Specifically, the judge weighs the seriousness of the offense committed by the worker and the violation of the right to privacy by the employer. In its judgment of 12 January 2016, the European Court of Human Rights (ECHR) considers that the control of e-mails and instant messaging of a worker does not violate the privacy of the latter. (Bărbulescu case v. Romania). The Court held that the fact that an employer wishes to verify that his employees perform their professional duties during working hours is not abusive. It also notes that the employer accessed his worker's account, believing that it contained communications from his worker with his clients.

In view of these developments above, NETIKA IT SERVICES IT Services wishes to inform its Clients who call to assist them in the control or to enter the mailbox of a worker, it will provide assistance while recalling the above-mentioned duties and procedure that all employers are obliged to bear the full costs incurred (administrative, legal, expert, advisory and other costs ...) in the event of a lawsuit or complaint against NETIKA IT SERVICES IT Services for breach of privacy a worker of his Employer client.

## Extract of Active Directory Policy

| Security Settings   |                          |
|---|--------------------------|
| Account Policies/Password Policy  |                          |
| Policy  | Setting                  |
| Enforce password history  | 3 passwords remembered   |
| Maximum password age  | 42 days                  |
| Minimum password age  | 0 days                   |
| Minimum password length   | 8 characters             |
| Password must meet complexity requirements                                    | Enabled                  |
| Store passwords using reversible encryption                                   | Disabled                 |
| Account Policies/Account Lockout Policy                                       |                          |
| Policy  | Setting                  |
| Account lockout duration  | 60 minutes               |
| Account lockout threshold   | 5 invalid logon attempts |
| Reset account lockout counter after   | 30 minutes               |
| Local Policies/Audit Policy   |                          |
| Policy  | Setting                  |
| Audit account logon events  | Success, Failure         |
| Audit account management  | Success, Failure         |
| Audit logon events  | Success, Failure         |
| Audit privilege use   | Success, Failure         |
| Account Policies/Kerberos Policy  |                          |
| Policy  | Setting                  |
| Enforce user logon restrictions   | Enabled                  |
| Maximum lifetime for service ticket   | 600 minutes              |
| Maximum lifetime for user ticket  | 10 hours                 |
| Maximum lifetime for user ticket renewal                                      | 7 days                   |
| Maximum tolerance for computer clock synchronization                          | 5 minutes                |
| Local Policies/Security Options   |                          |
| Network Access  |                          |
| Policy  | Setting                  |
| Network access: Allow anonymous SID/Name translation                          | Disabled                 |
| Network Security  |                          |
| Policy  | Setting                  |
| Network security: Do not store LAN Manager hash value on next password change | Enabled                  |