DIGIPLEX STOCKHOLM 1

FACILITY SECURITY MANUAL

The Site Procedures Governing Physical Security
at the DigiPlex DS1 Data Centre at Upplands Väsby

FUTURE
READY
IT-HOUSING

Contents

1.0 Introduction 3
2. On-Boarding and Off-Boarding 3
2.1 On-Boarding 3
2.2 Change of Personal Details 4
2.3 Off-Boarding 4
2.3.1 Immediate Termination 5
3. Security Card Issue 5
3.1 Security Card Request and Issue 5
3.1.1 Collection of Security Card 6
3.2 External and Internal Security Card 6
3.3 Replacement Cards 7
4. Visitors 7
4.1 Visitor Vehicle Parking 8
5.0 Security Access Areas 8
5.1 Access Areas Controlled by PIN 9
6.0 Recertification 9
6.1 Security Card Recertification 9
6.2 Recertification of Access Area Approvers and Recertifiers 10
6.3 Access Area Recertification 11
7.0 Vehicle Access 12
7.1 Deliveries and Service Access 12
8 Loading Bay 14
9 Parking 15
9.1 Vehicle Parking for Card Holders 15
9.2 Disabled Parking 15
10.0 Pedestrian Access 15
11.0 Emergency Services Access 16
12.0 Legal Right of Entry 16
13.0 Incident Management – Emergency Access 17
14.0 Planned Works (outside core hours) 18
15.0 Key Management 18
16.0 Mail Delivery and Screening 19
17.0 Bomb Threat 19
Appendices ..... Error! Bookmark not defined.

1.0 Introduction

This document details the standard operating procedures for the DigiPlex site DS1 in Sweden. Core hours for this site are: 08:00 – 18:00 Monday to Friday and the site has a 24/7/365 on site security presence.

These procedures are in accordance with the DigiPlex standards and security policy and are to be practised by all personnel.

There may be occasions when local processing or instruction from a guard differs from the Physical Security Manual standard, in such an instance the local instruction takes precedence and should be followed.

Reasons for local instruction/variations include:

- Response to an event or incident
- Regulatory and legal requirements.
- Physical design rework
- Technology or equipment service or breakdown

Where a Duty Holder title is shown in bold in the text, for example – **Security Manager,** details of all duties of the holder can be found in the Duty Holders Reference Document in Appendix A

2. On-Boarding and Off-Boarding

2.1 On-Boarding

All personnel requiring a DigiPlex security Card to access site must first be on-boarded.

The first stage is for the Card holders company to perform the agreed security clearance checks, in line with standards. Once completed the Card holder can be on-boarded by DigiPlex as below:

- The Card holder's **Company Card Sponsor** sends request by email for on-boarding to the **Security Manager**, details to include:
    - Card Holder Full Name (as shown on government issued ID)
    - Card Holder Company Name
    - Permanent or Contract Employee
    - If contract, expiry date for site access
    - Email address and contact Number
    - Declaration that the DS1 Site Induction for the individual have been completed and returned with a positive result

- The **Security Manager** will be responsible for accepting the request and once approved inform the Requester and Site Security about the approval.
- Once the approval is issued a request can then be raised for a security Card.

2.2 Change of Personal Details

Changes to a Card holder's details or circumstances will be reported to ensure all records are accurately maintained, examples of such changes include:

- Change of Name
- Criminal Conviction
- Change of Role/Sponsor
- Leaver (use the Off-Boarding process)

When such a change occurs, it is the responsibility of the Card holder or their **Line Manager/Sponsor** to ensure DigiPlex are advised as follows:

- Details of the change are emailed to the **Security Manager**, to include:
  - Change type
  - Change details i.e. Current name and new name
  - Employee ID
  - Date of change
- The **Security Manager** will update the records accordingly and where required will advise of any further action e.g. new security Card required
- Where the request relates to a leaver the Off-boarding process will be followed.

2.3 Off-Boarding

When a leaver is known the **Security Manager** will be notified as follows:

- The Card Holder or **Line Manager/Sponsor** will contact, by email, the **Security Manager** with the below detail:
  - Leavers name
  - Leaving date
  - Leavers ID
- The Card holder's access control record will be updated accordingly and an expiry date added, meaning the security Card will deactivate upon this date
- It is the responsibility of the Card holder to hand their Card to reception/security team on their last day

2.3.1 Immediate Termination

If an individual leaves employment through disciplinary action or without notice, the **Security Manager** must be notified immediately to suspend the individuals Card:

- Card Holders **Line Manager/Sponsor** should contact immediately the **Security Manager**
- The **Security Manager** will deactivate the security Card with a note stating reason for deactivation and date of action
- The security Card should be handed back to reception or security
- If the individual is deemed an ongoing risk to DigiPlex and this site, an image of the individual should be printed and stored at both reception and in the Security Control room for identification purposes. The image should include details of the individual and who to contact if access is attempted.

3. Security Card Issue

3.1 Security Card Request and Issue

Following successful completion of the on-boarding process, all personnel attending site, irrespective of organisation, must apply and have approval for a security Card prior to their first visit:

- The requester will need to complete an Access Card Application Form (Appendix A) and send to the **Company Card Sponsor** for approval.
- After approval, an updated Access List will be sent by the **Company Card Sponsor** to the **Security Manager** by email. After approval from **Security Manager** the Access List is sent to Site Security with a copy to **Company Card Sponsor** for knowledge.
- The requester will need to confirm all access required, along with the duration and ensure the relevant authorised access area approvers have approved prior to sending it to the **Security Manager**
- Site Security will check the authorised signatories and process the request accordingly
- A confirmation email will be sent to the requester, once processed with details for collecting the Card

3.1.1 Collection of Security Card

The Card holder will attend site for the first time as a visitor and during this visit the Card will be issued with allowed access within the site according to the approved access:

- Site Security will request visibility of the Card holders Government issued ID:
  - Current valid Passport
  - Current photographic Driving License
  - Current photographic National Identity Card
- Once verified a photograph will be taken of the Card holder and the Card is printed
- The Photograph will be taken against a blank background of head and shoulders, no hats, sunglasses or any item of clothing that may negate identification should be worn
- Prior or as a minimum during the visit the new Card holder will receive a site induction
- Following completion of the site induction the security Card will be issued for immediate use
- The Card holder need to sign the information with Rules for Access Card (Appendix G) prior receiving the Card.

Security Cards are issued and colour coded based on a number of criteria, a list of the different Card types can be seen in Appendix B. This allows easy identification of security Card types by all personnel whilst in the Facility.

3.2 External and Internal Security Card

Site access cards will have a zone 1 (External) access and can be used at the gates and into the reception area. All other doors are located within zone 2 (Internal). When you present your card at the man trap reader the guard will need to approve zone 2 access before entering. After identification the guard will grant you access and you are now allowed access to zone 2. Please understand that you do not have access to zone 1 until you pass out through the man traps. This will change your access to zone 1 which you need to have to pass the perimeter gates.

- External – allows access through the perimeter pedestrian/approved vehicle access point and in to the reception, but not beyond.
- Internal – allows access to approved areas within the building.

3.3 Replacement Cards

The loss or misappropriation of a security Card must be reported immediately to ensure the Card can be deactivated and a new one issued:

- The Card holder will inform Site Security which will inform the **Security Manager** upon arrival to site that they require a new Card along with the reason:
  - Lost Card
  - Stolen Card
  - Forgotten
  - Card not Working
- Access to site will be managed as per a visitor with the individual contacting security via the intercom at the pedestrian/vehicle entrance
- The Card holder will be asked to verify their identity by providing Government issued ID:
  - Current valid Passport
  - Current photographic Driving License
  - Current photographic National Identity Card
- Once verified access will be granted and a new Card will be issued and the old one removed from the system

Customers will be charged in accordance with the Added Value Services in Appendix C for each replacement card reissued to their personnel or sponsored contractor, where the justification is lost, stolen or forgotten Card. First 10 cards are included in contract, rest will be charged on a quarterly basis.

The **Security Manager** will log all requests for a replacement Card, including the Card holder's full name, ID, line manager details, date and time of issue along with the justification. These records will be sent to the relevant DigiPlex commercial staff for cross charging to Customers.

4. Visitors

Site Security with a copy to the **Security Manager** should be advised, in writing of all visitors at least 24 hours in advance. Security will require the following information for each visitor:

- Visitor Name
- Visitor Company Name
- Reason for Visit
- Escort Name
- Date and Time of Visit
- Vehicle Registration

Upon arrival, the visitor should contact reception using the intercom located at the pedestrian/vehicle gates and provide confirmation as to their visit in line with the information provided above. Once verified the visitors escort will be contacted and the visitor will be allowed access to reception, Security will monitor the access point via CCTV at all times.

When at reception the visitor will be asked to provide a positive identity check by an approved Government issued photographic identification:

- Current valid passport
- Current Photographic Driving License
- Current Photographic National Identity Card

The visitor will be asked to register in the visitor system and after completed registration and positive identification the visitor Card will be handed out by the guard in the reception. Details recorded on the Card will include:

- Name of visitor
- Escort name
- Arrival and departure times
- Vehicle registration number (if applicable)

It is the escort's responsibility to escort the visitor at all times and ensure they display their visitor Card.

4.1 Visitor Vehicle Parking

If a visitor is parking on site they need to enter their vehicle registration number in the visitor system.

5.0 Security Card Access Areas

Each designated area within the Facility will have an **Access Area Owner.** This duty holder can be a Digiplex or a Customer Senior Manager. Each **Access Area Owner** will submit below to Site Security:

- Those with delegated authority to grant access to his Area
- Those with delegated authority to recertify current access rights to his Area

When a requestor is compiling his Access Card Application Form, an authorisation is required for each access area for which he requests access to be added to his Security Card

Upon receipt of an approved access request Site Security will follow the below procedure:

- Verify the authorisers signature against the approved signatory list for the relevant access area
- If correct proceed with adding the required access to the Card and confirm to the requester when completed
- If any information on the form is incomplete/incorrect or the authoriser's signature is not valid, the request will be rejected and sent back to the requester. A reason for rejection will be included in the response to the requester.

5.1 Access Areas Controlled by PIN

Where an access area has a requirement for a PIN to be entered as well as a valid card read, the PIN should be allocated as follows:

- Upon validation of an access request with PIN requirement the Card holder should be contacted and a PIN agreed (four digits).
- This PIN should be input onto the access control system in line with the access area.
- If the Card holder forgets their PIN they can contact Site Security and upon validation of their identity can be advised of the PIN.

6.0 Recertification

6.1 Security Card Recertification

All Security Cards will require review and verification every 12 months:

- For each customer Site Security will run a predefined report from the access control system which details all active Card holders, to include:
  - Card Holder Name
  - Card Holder ID
  - Company Name
  - Expiry Date
- The report will be sent to the customer **Company Card Sponsor** who will review and return the report within 1 week, with a statement against each Card holder:
  - Valid
  - No longer valid – delete Card/off-board
  - Change of details – Confirmation of change
- Where a Card if no longer valid it should be deleted immediately
- Any changes recorded should be made accordingly

- The returned and completed report will be signed by the **Security Manager** and filed for 12 months.

Reports run for DigiPlex Card holders should follow the same process with the report being sent to the relevant **Company Card Sponsor.**

6.2 Recertification of Access Area Approvers and Recertifiers

All access area approvers and recertifies require recertification every 12 months:

- For each Customer Site Security will send a copy of the approved signatories list/access list for each access area and their recertifiers, to include:
    - Approver/Recertifier Name
    - Approver/Recertifier ID
    - Company Name
    - Access Area
    - Signature

- The report will be sent to the customer **Access Area Owner(s)** who will review and return the report within 1 week, with a statement against each approver/recertifier:
    - Valid
    - No longer valid – remove/off-board
    - Change of details – Confirmation of change and new signature

- Any changes recorded should be made accordingly
- The returned and completed report will be signed by the **Security Manager** once actioned and filed for 12 months.

Reports run for DigiPlex approvers and recertifiers should follow the same process with the report being sent to the relevant **Access Area Owner(s).**

6.3 Access Area Recertification

Access areas require recertification in line with the agreed timelines shown in the below table:

Access Area Type	Recertification Period	Recertification Completion By	Comments
All Card holders	Every 12 months	30 days	All Card holders, all space types. Customer will be charged as set out in Appendix C for mandatory annual review.

- For each Customer Site Security will run a predefined report from the access control system which details by access area all active Card holders with access, to include:
  - Card Holder Name
  - Card Holder ID
  - Company Name
  - Access Expiry Date
- The report will be sent to the relevant recertifer(s) who will review and return the report with a statement against each Card holder:
  - Valid
  - No longer valid – Remove Access
- Where access is no longer valid it should be removed immediately
- The returned and completed report will be signed by the **Security Manager** once actioned and filed for 12 months.

7.0 Vehicle Access

Unless the Agreement or other local circumstances do not allow, Card holders and visitors are allowed to enter the site with a vehicle. For visitor or extraordinary parking requests outside core hours the **Operations / Facility Manager** may be notified by the guard to make a decision and grant permission for the parking.

7.1 Deliveries and Service Access

The DigiPlex Site Security team will maintain an electronic diary of expected deliveries, services and collections which will require vehicle access through the site perimeter.
When arranging a delivery the requester must contact the Site Security team with 48 hours' notice of the delivery / collection with the following info:

- Date and time slot of delivery / collection
- Name of sender (Company or individual)
- Name of transport company / courier
- Name of receiver / attendee -who at DS1 will attend the delivery / collection (and be responsible for onward move of goods to final location within a specified timeframe)
- Alternative contact name and number in case the receiver / attendee cannot be contacted
- Size / weight of goods
- Will the goods need to be received at the Loading Bay? (Goods >20kg, or larger than a briefcase or small tool bag to go to Loading Bay).
- Requests received with less than 48 hours' notice will be rejected unless approved by the **Operations / Facility Manager** i.e. incident management

Upon arrival at the vehicle gate the process is as follows:

- The driver will contact security via the intercom at the vehicle gate and verify their identity by showing a Government issued photo ID, reason for visit and person taking receipt of delivery/collection
- The security team will verify the delivery using CCTV and the electronic diary
- The receiver / attendee will be contacted and requested to attend as appropriate
- The vehicle will not be approved for entry without the receiver / attendee first being contacted and available
- Upon validation of delivery the perimeter gate will be unlocked and the driver will access the air lock. Once the first gate is secure the second gate will be opened by security and the vehicle directed to the appropriate location

- Large trucks or lorries will not fit the airlock and Site Security will override the normal airlock with opening both gates to allow access
- Security will maintain visibility of the vehicle at all times whilst on site using CCTV
- Any vehicle that requests access that cannot be validated will be refused entry

.

The below table details types of delivery, access area and duty holder responsibilities:

Goods Type	Location	Who attends & Duties
>20kg, exceeding size limit or requiring mechanical aid for transfer within building	Loading Bay	Security Guard • Unlocks / locks roller shutter • Protects building from unauthorised entry Named Receiver / Attendee • Checks delivery / collection and signs for goods • Removes surplus packaging to appropriate waste bin • Organises onward transfer within building
Waste collection	Loading Bay	Security Guard • Unlocks / locks roller shutter • Protects building from unauthorised entry Named Receiver / Attendee • Checks collection and signs for service
Packages <20kg and less than size limit: Courier delivery / collection	Reception	Security Guard (within Sec office) • Manages access / egress courier to/from reception Named Receiver / Sender • Accept or dispatch package and sign with courier
Bulk delivery (fuel or similar)	Fuel Storage or similar point within grounds	Security Guard (within Sec office) • Monitor vehicle via CCTV Named Receiver / Attendee • Unlock / lock fuel store (or similar) • Accept and sign for delivery

Vehicle Egress process is as follows:

- The driver will contact security via the intercom at the vehicle gate and request exit
- Security will unlock the first gate and allow access to the air lock
- Once the first gate is secure the second gate will be opened by security for vehicle egress
- Large trucks or lorries will not fit the airlock and Security will override the normal airlock with opening both gates to allow egress

8 Loading Bay

Personnel arranging goods deliveries should ensure the vehicle access procedure for the site is followed (Section 7).
Following successful access to site the driver will be met at the Loading Bay by the arranged receiver / attendee and when needed the security guard, in accordance with the delivery booking. All deliveries/collections received by Site Security are tracked with electronical logging system.

No deliveries are to be stored in the Loading Bay area. Once unloaded goods / equipment should be moved and stored in the appropriate location.

If no designated area the unpacking should be done in the Loading Bay.

The Loading Bay operates on an interlock system which means the inner door, allowing access to the building, cannot be opened whilst the shutter is open. Security will monitor the Loading Bay via CCTV for the duration.

Once a vehicle has been unloaded/loaded it is to leave site immediately.

9 Parking

9.1 Vehicle Parking for Card Holders

The site has 43 parking spaces, 2 of which are designated for disabled drivers. Spaces will be allocated on a first come first served basis for Card holders. Security Card holders who are based at DS1 will be able to apply for a parking permit as follows:

- Card holder will apply for a permit using the Parking Permit Request Form (Appendix F)
- The detail required includes:
    - Vehicle Registration
    - Vehicle Make/Model and Colour
- Nothing larger than an SUV will be accepted
- The form will be sent to the **Operations / Facility Manager** who will review, and if approved, issue the permit.
- The permit must be clearly displayed in the vehicle at all times whilst on site.
- Once permit is approved, the Card holder can access site via the vehicle gate by swiping their Card on the reader and entering a valid PIN located at the gate

9.2 Disabled Parking

Any requests for disabled parking by security Card holders should be made using the parking permit process above, and highlighting the requirement for disabled parking. In all other aspects of a request, the process in Section 9.1 above will be followed.

10.0 Pedestrian Access

Security Card holders not parking on site will access through the designated pedestrian access point which is an interlock system, meaning the second gate will not open until the first is secured:

- The Card holder will swipe their Card on the card reader and enter a valid PIN at the first gate and access the interlock
- Once the first gate is secure they will swipe their Card on the second gate for access
- If the Card holder has an access issue or lost/stolen/forgotten card, they should contact security using the intercom and follow the visitor process

11.0 Emergency Services Access

In the event that the emergency services require access to site the security team should manage the situation accordingly:

- Whenever possible, all incidents requiring the attendance of emergency services should be notified to the Site Security team who will contact the appropriate emergency services. This ensures the security team is aware of the visit and can manage access appropriately
- Upon arrival security should verify the identity of those attending and allow access
- Where a vehicle cannot use the vehicle trap i.e. Fire Engine, both gates will be opened to allow access
- If possible Security will dispatch an officer to meet the emergency services at the vehicle gate and direct them accordingly
- Security should monitor the area on CCTV for the duration of the visit
- The incident should be logged by security and escalated to the **Operations / Facility Manager** and **Security Manager**.

12.0 Legal Right of Entry

Any legal search of any DigiPlex premises could significantly disrupt business and pose a threat to operational effectiveness. The following procedures apply in such cases.
All site management and security personnel, as well as reception staff will be made aware of appropriate action as a part of their duty training.
Where the request to access DigiPlex premises comes from a court or other official body the process is:

- Ask the visitors to identify themselves and to show their credentials, including the Warrant or Court Order, and the name of the organisation for which they are acting
- Ask the visitors to remain until advice is received. Never leave visitors unattended.
- Call the **Security Manager** emphasising the need for urgent advice. Do not leave a message; contact the next line of report, if necessary.
- In all such situations, Head Office must be informed immediately.

The **Security Manager** takes the following steps (these steps also apply to any DigiPlex site under construction):

- Alert building security to arrange direct assistance
- Comply strictly with the terms of the Order and permit access for the search to be carried out. It is important to ensure that the searchers also comply strictly with the terms of the Order.

- The person or persons conducting the search must be accompanied at all times.
- Keep a record of everything that is done. Note any instances where it is considered the searchers have exceeded their permitted authority.
- Ensure that all searchers are escorted off site.
- Do not comment to journalists or respond to any other outside enquiry regarding the Order or the search.
- Ensure that Head Office is fully informed.

13.0 Incident Management – Emergency Access

DigiPlex operate an incident management process which allows for access to site for personnel not in possession of a security Card. This could also include a delivery and vehicle access.
The **Operations / Facility Manager** will provide security with an approved signatory list of personnel who are authorised to act as **Incident Manager**, and to request access in an emergency. The **Incident Manager** will notify Site Security as soon as possible providing the following information:

- Visitors full name
- Company name
- Incident reference
- Estimated time of arrival
- Vehicle registration and vehicle type (if possible)
- Confirm whether or not a delivery of equipment will be required and whether this will be via the Loading Bay
- Confirmation if security escort is required or if a Card holder from the incident management team will act as escort. Escort details should be provided.

Where possible all requests for emergency access should be in writing, telephone calls will be accepted and must be followed by a written request.
Upon arrival to site the visitor will access site in line with visitor access procedures provided in this document.
Security will log all access in the daily occurrence log book

14.0 Planned Works (outside core hours)

All planned works by contractors or others, outside of core hours, must be approved via the Permit to Work system and Site Security notified in writing at least 48 hours in advance. The following information is required:

- Contractor/employee name
- Company name
- Permit to Work reference
- Date and time of visit
- Vehicle registration

Relevant site procedures should be followed for access.

Security can request visibility of a permit to work at any time whilst on site and approved permits must be provided when requested. Anyone found to be working without a valid permit will be asked to stop work and leave site. In such an instance Security should:

- Take details of the individuals on site, including their name, company name, works being undertaken, date and time
- The **Operations / Facility Manager** responsible for the work should be contacted immediately and advised of the situation

15.0 Key Management

Key issuance is managed using an electronic key management system located at Site Security.
If an individual requires access to a key they will need to apply for access to the electronical key logger in line with the security Card access area procedures.
Once access has been granted the process for accessing a key is as follows:

- User swipes card on the reader and enters valid PIN which will open the electronical key logger
- The approved key will be highlighted and can be removed
- Once the user has finished they should repeat the process and return the key in the highlighted slot

Any lost keys should be reported immediately to security and arrangements made for replacement lock barrels and keys.
A weekly key audit will be undertaken by Security, the audit should be logged with any missing keys reported and site procedures followed for replacement.

16.0 Mail Delivery and Screening

The volume of mail delivered via the Postal Service is expected to be comparatively low. Business related mail will be accepted at the site, and will undergo a fingertip / visual screening process carried out by the security team, before being distributed accordingly.
Employees must not have personal couriered deliveries sent to site. They will not be accepted via the procedures in Sections 7 & 8.

17.0 Bomb Threat

In the event of a bomb threat being received by phone, the person taking the call should use the Bomb Threat call check list (Appendix D) to guide them through the conversation and log as much information as can be obtained.
The **Security Manager** must be contacted immediately to alert them to the incident and the police called and their instructions followed.