Table of Contents

1.0 Introduction

This procedure details the security requirements that must be adhered to by all personnel working on or entering the site. These procedures are aligned to the DigiPlex Physical Security Policy and failure to comply could result in disciplinary action or removal from site.

DigiPlex's primary concern is for the safety and protection of people, assets and information.

To achieve this and ensure any security incidents are managed quickly and efficiently, the site security consists of a number of integrated security arrangements including:

- Manned Guarding
- Closed Circuit Television
- Pre-Authorised Access Procedures
- Electronic Access Control,
- Surveillance and Audit Trail Information
- Physical Barriers such as Fencing

2.0 Responsibilities

All employees, contractors, agency staff are required to comply with this Policy.

Line managers are responsible for monitoring compliance and providing guidance to staff on the implementation of the policy.

DigiPlex will take appropriate measures to remedy any breach of this Policy through the relevant framework in place. In the case of an employee, then the matter may be dealt with under DigiPlex's disciplinary process. Internal reviews by management and Internal Audit, including spot checks will take place in order to identify potential breaches of this policy.

3.0 Security Pass Management

The management of access is effected via a combination of paper processes and access control system.

All access must be applied for using the Access Request Form

- Access Card Application for Employees ULVEN, SEC-PROC-01-01-DGS
- Access Card Application Contractors ULVEN, SEC-PROC-01-02 –DGS
- Access Card Application for Employees ROSENHOLM, SEC-PROC-01-03-DGS
- Access Card Application for Contractors ROSENHOLM, SEC-PROC-01-04-DGS

Each access controlled area will have an owner who is responsible for providing an approved signatory list which is held in the Security Team. Signaturrett for DigiPlex, adgangskortsøknader, SEC-PROC-01-05-DGS.

All access request forms should be filed and securely stored in the security control room.

3.1 New Applications

Prospective access card holders are required to complete an access card application form for themselves, this is then validated and signed by one of those customers with authority to approve access to customer modules. For DigiPlex Employees, this is approved by the Line Manager and authorised by a Senior Manager within Operations. The completed form is then returned to reception for processing.

Completed applications are checked for completeness and accordance with the specimen signatures held. The prospective access card holders details are entered on the AIMS database, and access levels are set in accordance with those indicated on the access card application form. Customers are asked to allow two working days for this process.

Prospective access card holders are required to collect their access cards in person when valid photographic ID must be shown. A photograph of the card holder will be taken for to complete the database record. A new key card will be printed complete with a photograph and will be activated on the access control system.

Card holders must read and sign a copy of the rules of use related to holding an access card.

Card holders are required to display their cards whilst in the facility.

3.1.1 Additional Customer Security Clearance Requirements

DigiPlex understands that customers may have additional and enhanced requirements for security clearance levels. Where such a requirement exists, it will be the responsibility of the customer to complete these checks and ensure all personnel have the required level prior to requesting a authorizing a security pass from DigiPlex.

3.2 Change to Pass Holder Details

Changes to personnel's details or circumstances must be reported to DigiPlex HR department in order to update their records, this will include:

- Change of Name
- Change of Role/Line Manager
- Date of Change

Where such a change may result in further action such as a new or revoked security pass Line Managers are to advise security.

3.3 Leavers Process

Names and personnel ID's of security pass holders who are leaving the employment of DigiPlex or its customers must be given to security, who will add an expiry date and time to the security pass which reflects the last day of employment.

It is the responsibility of the Line Mangers to obtain employees ID Pass and return them to the onsite Security Team when they have left employment.
If an individual leaves employment through disciplinary action or without notice, security must be notified immediately to suspend the individuals pass.

Any individuals thought to be an ongoing threat to DigiPlex should report to the next shift and all security personnel made aware. If the individual tries to access any site they should be refused access and the incident reported accordingly.

3.4 Types of Passes

Security passes are issued and colour coded based on a number of criteria. The table below details the types of cards and the access requirements for each prior to issue:

Personnel Type	Access purpose	Card Type	Expiry	Access Arrangements	Additional Comments
Permanent DigiPlex Staff	Site Based	Permanent DigiPlex Site Pass	Permanent unless changing Role or leaving the Company	Permanent approved access Access approved by authorised signatory.	Must hold current site induction.
Customer Staff & Customer Contractors	Non-Site Based – Periodic Visits	Customer Site Pass	Permanent unless notified by Customer	Permanent approved access. Access approved by authorised signatory.	Must hold current site induction

Permanent DigiPlex Staff	Non-Site Based – Periodic Visits	Permanent DigiPlex Pass	Permanent unless changing Role or leaving the Company	Permanent approved access. Access approved by authorised signatory.	Must hold current site induction.
DigiPlex Approved Contractor	Ad hoc visits for planned service	DigiPlex Contractor Pass	Expires at end of visit	24 hours' notice of visit to be given to site security. Access approved by authorised signatory.	Must hold current site induction. Must have signed Declaration on Code of Conduct for Specialist Suppliers and Contractors.
DigiPlex Approved Contractor	Long Term site works	DigiPlex Contractor Pass	Expires after 6 months	Temporary approved access. Access to construction sites should be managed as per the site instructions	Must hold current site induction. Must have signed Declaration on Code of Conduct for Specialist Suppliers and Contractors.
All other visitors	Escorted Visits	Site Visitor Pass	Expires at end of visit	24 hours' notice of visit to be given to site security and approved by site manager (No card access given).	Visitor to have site induction and be escorted by approved host at all times.

In order to ensure that all security pass holders and their associated access remain valid it is important to regularly recertify both the person and access.

3.4.1 Permanent Employees

- All permanent DigiPlex employees will be issued with a photo ID security pass. This pass will give restricted access only where needed. To help identify permanent employees, the issued pass will be colour coded in accordance with DigiPlex policy.

- All requests for passes must be submitted to the Security Team using the Security Pass Application form with the appropriate line manager's authorisation. All forms without the correct authorisation will be returned to the originator and pass issue denied.

- Requests for access into operational areas such as customer modules, meet-me rooms, store rooms and other areas deemed sensitive by the appropriate

line manager/person responsible for the area will be restricted to those with a legitimate right to access these areas.

- All pass holders are permitted to take their pass off site at the end of each day. The table above details the security pass expiry periods for each personnel type.

3.4.2 Contractors

- All contractors with an approved Security Pass Application form will be issued a photo ID security pass. To help identify contractors, the issued pass will be colour coded in accordance with DigiPlex policy.

- All requests for passes must be submitted by the contractors sponsor to the Security Team using the Security Pass Application form with the appropriate line manager's authorisation. All forms without the correct authorisation will be returned to the originator and pass issue denied.

- Each pass issued will be programmed with access levels and expiry dates as appropriate.

- All pass holders are permitted to take their pass off site at the end of each day.

- Where long term construction works are planned, an ad hoc process may be agreed between all parties. This process must be approved by the DigiPlex Security Manager and assignment instructions produced for the relevant site for the duration of the works.

3.4.3 Customer Employees

- During establishment of a new Customer Agreement specimen signatures of those with authority to approve access to customer modules is established. If customers need to vary this, new specimen signatures and declarations are obtained.

- Prospective access card holders are required to complete an access card

application form for themselves, this is then validated and signed by one of those customers with authority to approve access to customer modules. The completed form is then returned to reception for processing.

- Completed applications are checked for completeness and accordance with the specimen signatures held. The prospective access card holder's details are entered on the AIMS database, and access levels are set in accordance with those indicated on the access card application form. Customers are asked to allow two working days for this process.

- Prospective access card holders are required to collect their access cards in person when valid photographic ID must be shown. A photograph of the card holder will be taken for to complete the database record. A new key card will be printed complete with a photograph and will be activated on the Access Control System.
- Card holders must read and sign a copy of the rules of use related to holding an access card.
- Card holders are required to display their cards whilst in the facility.

3.4.4 Visitors

The management and registration of visitors is undertaken via the Visitor database system. To enter the facility visitors must be escorted by an access card holder.

Visitors are required to self-register using the approach and use terminal on the Reception counter, on completion a self-adhesive ID label is produced behind the reception screen or at the counter. A cardholder is required to follow the Visitor.

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

Visitors are not permitted to use any device to take images in any part of DigiPlex sites. Anyone caught doing so will be escorted from the site and images deleted.

3.5 Security Pass Re-verification

All Security passes will require review and verification at least every 12 months, the Security team will collate and send reports to line managers/customer representatives who will recertify the personnel reported and respond to the Security Team within one week.

The response should include any changes to details as shown on the report, verification that each individual is still an employee/contractor for the company and that a security pass is still required.

The Security Team will apply any updates required and delete any security passes along with associated access that is no longer required. All reports and responses will be stored by the Security Team for a minimum of 12 months.

4.0 Awareness

The following principles should be applied on all DigiPlex sites:

- Never leave external doors unlocked or unattended
- Never allow access to strangers without a formal check
- Always politely challenge unaccompanied visitors or people not displaying a pass
  Do not assume that because a person is in possession of a valid building pass that he/she has the authority for onward entry into a sensitive area.

In addition, Card holders, will be provided with the following information

- When entering your PIN code, be sure to hide it from others.
- Do not give other people access to the DigiPlex facility & site.
- Your access card is personal and your movements are recorded such as your move throughout the facility.
- Always keep your card visible when in the facility.
- Lost or stolen access card must immediately be reported to Digiplex, phone no. +47 23 20 78 60 or e-mail security.dnas@digiplex.com access card will be invalid.
- Guests must be registered using the self-registration system Visitor and must be escorted by an access card holder at all times even during silent hours.
- Violation of rules on use of access cards can and will lead to confiscation of cards.

See SEC-GUI-01-01-DGS Rules for access card holder DNAS, See SEC-GUI-01-02-DGS-Rules for access card holder DRAS.

5.0 Escort Requirements

Escorts must be permanent security pass holders and have the appropriate access for the areas being visited. Escorts are responsible for their visitors from their admission into and until their departure from all DigiPlex buildings.

It is the responsibility of the escort to ensure that all visitors issued with a visitor pass display it at all times whilst on DigiPlex premises. The escort must also ensure that the pass is returned to reception on leaving and that the visitor is 'signed out' as appropriate.

Escorts must collect all visitors from the reception and escort them until they leave the building or another escort accepts responsibility for them. They must ensure that visitors are escorted from the site and not left to roam buildings.

All visitors who are not in the company of a DigiPlex employee should be politely challenged and taken to reception or security and the incident reported to the security team.

6.0 Replacement Passes

The loss or misappropriation of a security pass must be reported immediately to security and the employee's line manager. The card will be deleted from the access control system and a new one issued upon approval.

Personnel who forget to bring their pass to site will be required to book in as a visitor and treated in the same way by being escorted.

Personnel who forget to bring their pass can be given a loan card for the single visit.
The Security guard will by the access control system check the permanent valid access card before any loan card is given. Loan card application must be filled in by the applicant.
The loan card must be returned to the reception at the end of visit.

7.0 Responsibilities of Security Pass Holders

All personnel entering DigiPlex buildings will display their issued security pass at all times whilst on the premises and produce their pass when requested by security or another member of staff.

- The security pass will be displayed at or above waist height.
- All personnel have a responsibility to question anyone not displaying a valid security pass.
- All staff must ensure that unauthorised personnel do not gain admission to access controlled areas without use of their own pass.
- Any member of staff who permits another person to use his/her pass for access will be subject to disciplinary procedures.

8.0 Access of Areas

Each access area within a DigiPlex site, including customer space, will have an owner assigned. It is the owner's responsibility to ensure that no unauthorised access is approved for his/her space. In order to achieve this they will assign access area approvers and access area recertifies.

Access into all restricted or sensitive areas must be firstly verified by the employee's line manager and the authorised approver for the area using the Access Request Form.

The access area approvers will be responsible for the approval of all access requests by signing any valid request forms. A full list of authorised signatories will be kept by the Security Team.

Access area recertifies have the responsibility of ensuring that all access currently applied to security passes is valid. This is achieved through regular checks, the frequency of which has been pre-determined by DigiPlex and is based on the type of area along with its sensitivity.

At least every 12 months the Security Team will send a report to the area owner detailing the current area approvers and recertifies. The area owner must review and respond with any amendments, removals or additions within one week.

The Security Team will make any requested amendments and store the report and responses for a minimum of 12 months.

This table details defines the zoning, area owner and their recertification period:

Access Area Type	Recertification	Recertification Completion By	Comments	Area Owner
DigiPlex Office Staff	N/A	N/A	General access areas include: Perimeter entry, office and main corridors to office only.	Line Manager
DigiPlex Management	Every 12 months	10 days	As above and all general areas and corridor without modules.	Operations Director Norway
DigiPlex Operations	Every 6 months	5 days	Full Site Access	Head of Operations
DigiPlex AVS	Every 6 months	5 days	DigiPlex Management and CCR Rooms	Operations Director Norway

For those restricted/sensitive areas that are secured manually, the keys will be secured in an electronic key press. These keys can be accessed by approved security pass holders only.

9.0 Access Outside of Normal Working Hours

Core business hours are 08:00 – 16:00 Monday to Friday, except Bank Holidays/public holidays.

Any planned works by contractors or others outside of normal working hours should be approved via the Permit to Work system and security notified in writing at least 48 hours in advance. Security will require the following information:

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

The contractor must have a hard copy of the approved permit on arrival. Access will be added to the individual's security pass for the time permitted by the permit or a security escort provided if requested.

All personnel wishing to gain access to buildings outside of normal working hours will be required to sign in and out as described above.

10.0 Emergency Access

In the event that emergency access is required, such as an IT engineer working on an urgent server outage, access will be granted in accordance with the approved incident management process.

All access in an emergency must be escorted by either an approved escort or security. The escort is responsible for staying with the visitor at all times.

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, the engineer must report to reception and will require a positive ID check using one of the following forms of Government issued photographic ID:

- Current Passport
- Current photographic Driving License

A visitor badge will be issued and if requested Security will provide an escort or contact the confirmed escort.

11.0 Key Management

Keys are used to secure certain doors to areas not generally available to customers. Keys are held in a "key watcher" within the reception area

Keys may be loaned on a temporary basis to directly employed staff and contractors when needed. Keys are signed out by persons with authority to enter the key watcher. All activities are logged with names, date and time.

All keys should be returned by 16:00hrs each day and Keys will not normally be loaned overnight. Where keys must be loaned overnight. The person has to clarify with Digiplex reception.

A log is pulled out every afternoon. With unreturned keys, the person will be notified by the reception security guard.

The master key will not be loaned. If the master key is need for any reason an authorised employee of DigiPlex shall escort the person needing access.

Any missing keys should be reported immediately to security and arrangements made for replacement lock barrels and keys.

12.0 Goods Delivery

Customers and contractors may at their own discretion arrange for packages to be shipped directly to the facility for later collection and incorporation.

Customers are asked to nominate a single point of contact for notification in the case of goods receipt, and to give two working days' notice of large package deliveries.
Each package/delivery is registered with SendSuite Tracking scanner which email customer with a notification that a delivery has arrived.

The received goods are stored in a locked storage room until they are collected. Goods that are too large to be moved/stored are placed in a controlled zone such that they are monitored by CCTV until collected.
Customers are asked to collect goods within 3 working days.

13.0 Forms and Template

The following forms and templates are an integral part of this procedure.

Access Card Application for Employees ULVEN	SEC-PROC-01-01-DGS
Access Card Application Contractors ULVEN	SEC-PROC-01-02-DGS
Access Card Application for Employees ROSENHOLM	SEC-PROC-01-03-DGS
Access Card Application for Contractors ROSENHOLM	SEC-PROC-01-04-DGS
Rules for access card holder DNAS	SEC-GUI-01-01-DGS
Rules for access card holders DRAS	SEC-GUI-01-02-DGS

14.0 Records and Retention

Controlled documents that have been superseded or withdrawn will be archived as specified in the latest issue of the Control of Records procedure (QA-PROC-02-00-DGS).