ACCESS CONTROL MANAGEMENT

DigiPlex Group of Companies

CONTENT

1 Introduction

DigiPlex's prime concerns in operating its data centres are the safety and protection of people, assets and information. The effective security of, and access control to, each data centre site is critical in addressing these concerns. The detailed security procedures aligned to the access to DigiPlex data centres addressed below are to be strictly implemented. Failure to comply could result in disciplinary action or removal from the data centre site.

2 Scope

All DigiPlex employees, suppliers and customers are required to comply with the requirements in this document.

3 Security Arrangements

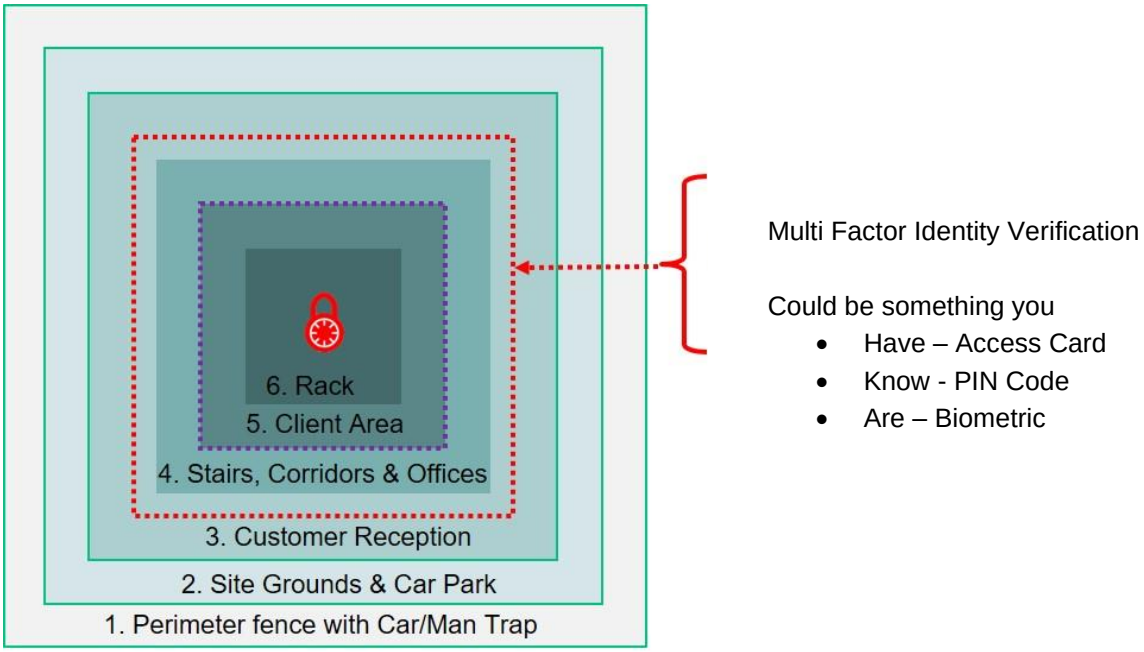
The specific security arrangements at each DigiPlex site may vary, but each site will have a multi layered integrated security system that will feature a combination of physical, technical or manned measures. The site's integrated security arrangements may consist of some or all the security arrangements below:

- 24/7/365 Site Security and Manned Guarding
- Manned Reception during Core Working Hours; Monday to Friday
- 'Man-Trap' access to data centre secure area
- Security policies, procedures and instructions
- Physical Barriers such as perimeter fencing with the intention to Deter, Detect and Delay unauthorised access.
- Vehicle gate operation and management
- Hostile Vehicle Mitigation measures
- Access Control System with multi factor identification that may include integrated biometric verification
- Intruder Detection System
- Random checks by security staff
- Closed Circuit Television (CCTV) with motion detection
- Security Lighting
- Audit

Each data centre is divided into 6 (six) distinct physical security zones

- S0 – Open – outside fence.
- S1 – Common Area – outside building but inside fence.
- S2 – Common Area – reception/access control/goods reception/unpacking
- S3 – Common Area in Building – stairs/lifts/other Common Area inside Building
- S4 – Gross Area in Building (technical preparations, corridors, storage, technical rooms)

- S5 – White Space
- S6 – Rack



4 Responsibilities

Personal responsibilities for physical security matters are:

Role	Responsibility
DigiPlex Head of Security	Overall accountability for Security Strategy, protocols and procedures within the DigiPlex Group of Companies
Operations Managers	Accountable for ensuring that Security Strategy, protocols and procedures are implemented at the sites for which they are responsible
Line Managers	Accountable for ensuring that their employees and contracted personnel understand the Security Strategy, protocols and procedures at the sites that they are working
Supplier Owner	Accountable for ensuring that their supplier chain understands and follows the Security Strategy, protocols and procedures at the sites that they are working
Customer Relationship Manager / Key Account Manager	• Accountable for ensuring that customers are aware of the Security Strategy, protocols and procedures as applicable to them are understood and followed for the sites at which they are located • Responsible for ensuring that any customer specific security requirements are understood by all stakeholders

5 Access Management

DigiPlex Data Centres are restricted access areas. Only persons with a need to access the data centre are allowed access. There are essentially two methods of access to the data centres

- As an authorised card holder
- As a pre notified visitor

DigiPlex uses a proprietary IT Service management System called ServiceNow. The management of access for all DigiPlex sites is executed through the ServiceNow Customer Portal.

All data centre access must be applied for using the Customer / Supplier services page in the ServiceNow Portal. The relevant Site Manager / OPS Manager holds the approval rights for DigiPlex staff and suppliers. Authorized customer representatives hold access authority to their customer areas.

5.1 New Access Card Applications

All new access card applications must be requested in ServiceNow by

- DigiPlex staff - Line Mangers or
- Supplier - Owner / Project Manager.
- Customer – Authorised Signature

Applications should be requested a minimum of 2 working days before the access card is required.

Access Card applications are approved by the relevant Site Manager / Operations Manager, through a workflow in ServiceNow. The Access Card Applicant receives an e-mail with Terms and Conditions which must be confirmed. In the same e-mail a link to the online Card Holder Induction training module is provided. The Induction gives important safety information about DigiPlex' datacentres and Access Cards are not issued before the Induction training is completed.

Completed applications must be checked according to the check list in the electronic application form. The prospective cardholder's details are entered to the Access Card database, and access permissions are set in accordance with those indicated on the application.

Prospective Access Cardholders are required to collect their access cards in person and a valid photo ID must be shown. A photo of the cardholder will be taken by the site Security team to complete the database record. A new access card will be printed complete with photo and will be activated in the access control system.
Access Cards must be worn on the outermost layer of clothing, and in a manner that it is visible between the neck and waist at all times when in the data centre, unless carrying out work where the wearing of and Access Card would compromise safety.

5.1.1 Additional Customer Security Clearance Requirements

DigiPlex understands that some 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 relevant persons have the required level of clearance prior to authorizing an access card from DigiPlex.

Relevant procedure reference:

- ***SEC-PROC-02-00-DGS Access to Customer Areas with their own external Access Control System***

5.2 Change to Access Card Holder Details

Changes to personal details i.e. change of name, must be reported to:

- Line Manager or HR department in DigiPlex if DigiPlex employee
- Supplier Owner / Supplier Contact in DigiPlex if supplier of DigiPlex
- Customer Representative with Signatory Right if employee or supplier of customer

Application for a new access card must be made in the Customer Portal with the new information. Old access cards to be cancelled in the Access Control system and the card destroyed by the Security team.

5.3 Leavers Process

When a cardholder leaves the employment of either DigiPlex, customer or suppliers of both, a Cancellation notification must be raised in the Customer Portal with requested information. This to be done by:

- Relevant Line Manager /HR if employee in DigiPlex
- Supplier Owner or Supplier Contact in DigiPlex if employee of long-term supplier of DigiPlex
- Customer Signature Right Holders if employee of customer or any of their suppliers.

Security receives the Cancellation notification and add an expire date for the card in the access system.

If an individual leaves employment through disciplinary action or without notice, Security must be notified immediately by phone to suspend the individuals Access Card. This in addition to the above-mentioned cancellation process.

Any individuals considered to be a threat to the security of a DigiPlex should be reported to Security who should ensure that all security personnel made aware. If the individual tries to access any DigiPlex Site, they should be refused access and the incident reported accordingly as a Security Incident in ServiceNow.

5.4 Types of Access Cards

Security passes are issued, and colour coded based on several 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 Approval	Additional Requirements
Permanent DigiPlex personnel	Permanent or periodic work at Site	DigiPlex Employee	Permanent unless changing role or leaving DigiPlex	Access approval by relevant Site / OPS Manager	Card Holder Induction
DigiPlex periodic supplier	Planned periodical service / work at Site	Supplier	Expires at end of planned work period	Access approval by relevant Site / OPS Manager	Card Holder Induction and Code of Practice for Suppliers. Change Request are required but exceptions can occur.
DigiPlex long term supplier	Long term work at Site	Supplier	Expires after agreed working period	Access approval by relevant Site / OPS Manager	Card Holder Induction and Code of Practice for Suppliers. Change Request are required but exceptions can occur.
Customer personnel and suppliers /contractors of customer	Periodic work for customer in customer areas	Customer Access Card	Permanent unless notified by Customer	Permanent approved access approved by customer representative with Signatory Right	Card Holder Induction
Visitors	Several reasons	Visitor card / badge to wear well displayed. Visitor card to be returned / badge scanned out when leaving.	Expires at end of visit	Permanent access card holder authorised to receive visitors	48 hours notification to of visit to be requested in ServiceNow. Visitor to be escorted at all time by the card holder.

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.

5.4.1 Permanent Employees

- All permanent DigiPlex employees will be issued with an access card holding a photo ID. The card will give restricted access where needed. To help identify permanent employees, the issued pass will be colour coded in accordance with the DigiPlex Visual Guideline kept by Marketing.

- All requests for access must be raised by Line Manager by filling in the electronical application in ServiceNow. The application will, through a workflow, be authorized by relevant Site Manager /OPS Manager and submitted to the Security Team for issuance of access card.

- Requests for access into operational areas such as customer modules, meet-me rooms, storerooms and other sensitive areas deemed sensitive will be restricted to those with a legitimate need to access these areas.

5.4.2 Suppliers

- All suppliers to DigiPlex will be issued with an access card holding a photo ID. To help identify suppliers, the issued access card will be colour coded in accordance with the DigiPlex Visual Guideline kept by Marketing.

- All requests for access must be raised by the DigiPlex employee engaging the supplier by filling in the electronical application in ServiceNow. The application will, through a workflow, be authorized by relevant Site Manager /OPS Manager and submitted to the Security Team for issuance of access card.

- Each access card will be issued with programmed access levels and expiry dates as appropriate for the engagement.

- All access cardholders are permitted to take their card off site at the end of each day.

5.4.3 Visitors

Anybody who is not an Authorised Access Card holder is considered to be a visitor. All visitors must be pre notified using the Notification Visitors service in the Customer Portal. All visitors are to be escorted by an Authorised Access Card holder at all times whilst in the data centre.

- Approved visitors are to present themselves to the Site Security; first via the gate intercom and then once admitted, in the reception to get their identification validated by comparison between received visitor notification and a valid photo ID-card presented by the visitor.

- The management and registration of visitors is undertaken via a database system. Visitors are required to self-register by using the visitor terminal in the reception where such a system is established. A self-adhesive visitor label or a visitor card is produced and must be worn on the outermost layer of clothing, and in a manner that it is visible

between the neck and waist at all times when in the data centre, unless carrying out work where the wearing of and Access Card would compromise safety.

6 Escort Instructions

All escorts must always be performed by Authorized Access Cardholders that hols the appropriate access for the areas being visited. Escorts are responsible for their visitors from meeting them upon arrival and until departure from the Site.

It is the responsibility of the escort to ensure that all visitors are issued with a visitor card or label and wear it well displayed at all times whilst on DigiPlex premises. The escort must also ensure that self-registered visitors are ‘signed out’ from the Visitor System when leaving or return the visitor card.

Visitors who are not accompanied by an Authorised Cardholder with the correct access should be politely challenged and taken to the Security. The incident is to be reported as a Security Incident.

7 Rules for Access Card Holders at all Datacentres

Access Card holders must ‘swipe’ in and out of all secure areas (areas with a card reader), and failure to ‘swipe in’ correctly will result in the generation of an alarm.

If multiple badges exist on a lanyard or badge holder, they should be isolated in order to reduce the opportunity for the badge to be misread.

If initially denied access (notified by a red LED, annunciator and beeping tone) on a badge swipe, the Access Card holder must:

- stop and contact site security
- only ‘swipe in’ again once instructed to do so
- refrain from badging more than twice or force a door open as this will cause an alarm

Access Card holders must not hold any door secured by a badge reader open for another individual. Such behaviour is known as “Tailgating” and is strictly prohibited.
Always wait for the door to fully close before trying to badge in or out of a door that was just accessed by another individual.

Access Card holders must not hold any door open for longer than 59 seconds – doing so will result in an alarm. If the door is required to be open for longer than 59econds, the Access Card holder must notify security.

Access Card holders should immediately enter/exit a cage after swiping their badge and receiving a green LED (annunciator and solid tone).

If an Access Card holder has forgotten something and/or they determined that they are not ready to enter/exit the cage, they will still need to enter/exit the cage and then enter/exit the cage appropriately – doing so will clear their badge and prevent alarms.

If an Access Card holder/visitor causes an alarm, they are required to stay at the module/cage until site security arrives. Site security is immediately notified of all alarms and will respond to the location of the alarm. The Access Card holder responsible for the alarm will be re-briefed on Access Card procedures, and the issue will be reported to the leadership team of the individual who caused the alarm.

Access Card holders that continue to cause alarms or do not follow these procedures may incur immediate and permanent/temporary revocation of facility/cage access privileges

Access Card holders are required to secure/protect their Access Card at all times, and failure to secure/protect an Access Card may result in immediate and permanent/temporary revocation of facility/cage access privileges and disciplinary actions by their employer

It is unacceptable to allow another individual to use an Access Card/PIN assigned to another Access Card holder and doing so may result in immediate and permanent/temporary revocation of facility/cage access privileges and disciplinary actions by their employer.

7.1 Abuse of Access Card Terms and Conditions

Abuse of the Access Card Terms and Conditions is considered to be a security breach and is to be reported as a Security Incident. Violation of rules on use of Access Cards can lead to removal from site and forfeiture of the card.

DigiPlex will take appropriate measures to investigate and remedy any security breach.

If the breach is by DigiPlex employee, the matter will be dealt with according to ***HR-PROC-01-01-DGS HR's Grievance Process and Procedure***.

If the breach is by a customer, the Authorised Signature will be notified of the breach and any action taken.

If the breach is by a supplier/contractor, the Supplier owner will be notified of the breach and any action taken.

7.2 Access Card Re-verification

Customer approved Access Cards can be reviewed by the Authorised Signature in the Customer Portal. Customers should review and verify their Access Card holders at least every 12 months. Any discrepancies identified should be reported to the relevant site security team through the Customer Portal.

8 Awareness

The following principles applies at all DigiPlex sites:

- Never leave doors unlocked which are not supposed to be open.
- Never allow access to strangers without following the formal procedure described in this document.
- Always politely challenge unaccompanied visitors or people not displaying a visitor label or access card.

Do not assume that because a person is in possession of a valid access card, they also have the authority to entry sensitive areas.

9 Replacement passes

The loss or misappropriation of an access card must be reported immediately by the owner to the local Security team or to DigiPlex by phoning +46 72 733 11 50 and to the:

- Employee's Line Manager, if an employee of DigiPlex
- Supplier responsible in DigiPlex, if a supplier
- Customer authority with signature right towards DigiPlex, if a customer representative

Lost card will be deleted from the access control system and a new one issued upon approval.

Personnel who forget to bring their access card can be given a Loan Card by contacting the Site Security. The Security check the access control system for existing valid permanent access. In addition, Security must obtain verification from the authorised access card approver for the person and check her or his valid photo ID-card. The Loan Card must be returned to the reception when leaving the site.

10 Access to Restricted Areas

Access to all restricted areas must be authorised by the person's Line Manager if an employee of DigiPlex or the Supplier Owner, if a supplier. A Change Request must be approved before any access authorisation is provided.

Access to restricted areas are only provided for technical personnel, Site Managers, OPS Managers and AVS Managers.

Where customers have their own Access Control systems, they are responsible for the Access rules for the areas under their control. DigiPlex personnel that are granted access to these spaces are to follow the customer rules for the space.

11 Access Outside Normal Working Hours

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

Any planned work by suppliers or others outside of normal working hours should be approved in the Change Management Process and Security notified through ServiceNow 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

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.

12 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 persons provided with emergency access in an emergency who do not hold permanent site access cards must be escorted by an approved escort as described in section 5.4.3. The escort is responsible for staying with the visitor at all times.

The Authorized Signature/ Customer NOC should notify security as soon as possible providing the following information:

- Engineer's full name
- Company name
- Incident reference

- Estimated time of arrival
- Vehicle registration
- Confirm whether or not a delivery of equipment will be required

Where possible all requests for emergency access should be in writing either by email or ServiceNow, 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 officially issued photographic ID:

- Current Passport
- Current photographic Driving License
- Current National Identity Card

A visitor badge will be issued and if requested Security will provide an escort or contact the confirmed escort. The engineer must sign in and out as described above.

13 Emergency Services Access

Emergency Services vehicles and personnel Fire, Police and Ambulance are be allowed access to the site in response to a callout by the site team.

14 Requests to Search Premises (Dawn Raid)

It is essential to ensure that government searches, search warrants or raids (also known as “dawn raids”) are managed appropriately. Each customer will have its own internal policy and procedures for managing a ‘Dawn Raid’. This section gives an overview of instructions issued to the site Security Team.

All site management and security personnel, as well as reception staff, are made aware of appropriate action as a part of their training.

The following procedures apply in such cases:

- Site Security will ask the visitors to identify themselves and to show their credentials, including the Warrant or Court Order, the name of the organization for which they are acting and the scope of the Warrant.
- The visitors will be asked to remain in the Reception Area until advice is received. Visitors will not be left unattended
- Security will call the DigiPlex Operations Manager or the next point of escalation if not available emphasizing the need for urgent advice.

In all such situations, DigiPlex Head of Security must be informed immediately.

The Operations Manager will:

- Verify the Scope of the Warrant and inform the Customer Authorised Signature for the area subject to the “Dawn Raid”.
- On arrival of the Customer Authorised Signature, support the customer to comply strictly with the terms of the Order and permit access for the search to be carried out.
- Not comment to journalists or respond to any other outside enquiry regarding the Order or the search
- Notify DigiPlex Senior Management

15 Goods Delivery

Customers and suppliers may at their own discretion arrange for packages to be sent directly to the Site for later collection and incorporation. This has to be pre-announced through DigiPlex’ Customer Portal a minimum 2 working days before expected arrival. The following information must be provided in the notification:

- Addressee company name
- Contact person within the company and phone number

Each package / delivery is registered by the Security and arrival notification is sent to the receiver’s contact person.

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 and must be monitored, preferable by CCTV, until collected.

16 Related Documents

- SEC-POL-01-00-DGS Physical Security Policy
- SEC-STR-01-00-DGS Security Strategy and Security Review 2019
- SEC-PROC-02-01-DGS Access to Customer Area with External Access Control System
- SEC-PROC-02-02-DGS Customer Signature Right Form
- OPS-PROC-05-00-DGS Change Management