Section Three – Description of DigiPlex’s system related to data center colocation hosting services throughout the period 01 January 2020 to of 31 October 2020

**Overview**

**Applicability & Purpose of Report**

The purpose of this report is to cover the description of the system of DigiPlex AS (the “Service Organization” or “DigiPlex”) related to General IT Controls for data center colocation hosting services provided to its clients (“User entities” or “User Organizations”) from DigiPlex data centers located at:

* DigiPlex Norway AS
* DigiPlex Rosenholm AS
* DigiPlex Fetsund AS
* DigiPlex Fetsund 2 AS
* DigiPlex Holtskogen AS
* DigiPlex Stockholm 1 AB
* DigiPlex Copehagen 1 ApS

**Business description**

At DigiPlex, we believe that the digital economy should be a green and sustainable economy. To help ensure this, we design, build and operate data centers that are cutting edge of environmental performance. We have been doing this for 20 years and have set the standard for sustainability in the sector. We will continue to lead and act as the role model for the industry.

DigiPlex is headquartered in Norway and currently operates eight data centers across Norway, Sweden and Demark , delivering best in class services to our global customers.

In the summer of 2021 DigiPlex was acquired by IPI Partners, LLC, a global investment platform focused exclusively on data centers and other technology and connectivity-related real assets (IPI). Through the transaction IPI acquired 100% ownership of all DigiPlex Group companies. 

**Vision**

We at DigiPlex are all committed to one common purpose:

**“Enable digitization by providing the most innovative, sustainable and secure data centers in the Nordic region.”**

**Integrity and Ethical Values**

Corporate governance at DigiPlex starts with the Executive Management Team (Board of Directors) that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at DigiPlex serves several purposes:

1. To establish and preserve management accountability to DigiPlex’s owners by appropriately distributing rights and responsibilities among the Executive Management Team, directors, managers, and shareholders.
2. To provide a structure through which management and the Executive Management Team set and attain objectives and monitor performance.
3. To strengthen and safeguard a culture of business integrity and responsible business practices.

**Values**

Trust, respect, honesty, transparency and professionalism are the foundation blocks of our relationship with everyone who interacts with our Company.  To achieve this, DigiPlex recognizes that the behaviors of all our employees must experience and deliver to the same high expectation, as this acts as the benchmark for our professional conduct.  Our reputation is built upon integrity, honesty and acting responsibly whilst respecting the Laws and Regulations, Traditions and Cultures of the work environments within which we all operate.

In support of our Company mission we are all committed to the following values:

|  |  |
| --- | --- |
| * **Customer Partner** | *to partner with our customers and ensure success by creating exceptional value through innovative solutions and services.* |
| * **Teamwork** | to work together effectively to achieve our goals, while encouraging individual engagement, contribution and responsibility. |
| * **Innovation focused** | *to create and sustain a culture where entrepreneurship is encouraged and rewarded.* |
| * **Personal accountability** | *to be empowered to embrace personal ownership for delivering on our commitments.* |
| * **Respect** | *to act with integrity and considerations towards all.* |
| * **Passionate** | *to be passionate about winning and about DigiPlex, our services, our people, and having fun, while delivering superior value to all stakeholders.* |

These define the way we run and aim to grow DigiPlex.  They set out the services we wish to provide, our behaviors and the way we manage our business.  Our values form the foundations from which our systems and processes are developed and ensure we are all committed to be working from a commonly understood base, that can be consistently applied across our Company.

**The types of services provided**

DigiPlex is a company providing highly secure high-powered, energy-efficient, carrier-neutral, co-location data center space in Scandinavia for our customers' information and communication technology (ICT) equipment.

Our approach ensures a cost-effective environment offering speed to market and inherent flexibility and scalability for the future.

* **Secure**: Our centers deliver several layers of security to organizations who require specialist environments for applications ranging from network operations through disaster recovery to data center space and secure printing.
* **Resilient**: DigiPlex also provides guaranteed continuity of power into and throughout our conditioned, chilled modules, suites and rooms supporting our customers as they ensure business continuity.
* **Connected**: Our secure centers offer multiple telecoms facilities underpinned by our commitment to independence and neutrality.

DigiPlex supports our customer's competitive quest for best value and best practice. The center is used by customers for applications ranging from disaster recovery through to frontline server space, and secure network control centers.

**The principal service commitments and system requirements**

DigiPlex has adopted a process approach in the development and implementation of its management system for the provision of services. The aim of the management system is to enhance customer satisfaction by meeting customer requirements. In addition, each of the processes undertaken is controlled to reduce the impact of the company’s activities and services on the environment and to eliminate or minimize Health & Safety and Information Security risks to its employees and other interested parties. Continual improvement of the effectiveness and performance of the management system and processes is attained through performance measurement and the achievement of objectives.

**The quality policy of DigiPlex**

Therefore, our reputation and capability to grow our business depends on our ability to provide products and services that are of a consistent, reliable and high quality, meeting or exceeding our customers’ needs and achieving customer satisfaction.

**We will:**

* Work closely with our customers to fully understand their needs and meet their expectations throughout the life of their contract with us.
* Set stretching objectives and targets which are focused on meeting the needs of our customers, our business and other stakeholders.
* Use all necessary resources – in a way that clearly allocates responsibilities relating to quality to appropriate staff – to make sure we meet the commitments we have made to our customers.
* Make sure our employees have adequate training and have the skills, knowledge and experience they need for their roles.
* Encourage effective teamwork and make sure staff feel empowered, accountable and understand how meeting their objectives will contribute to the success of their particular department and DigiPlex.
* Measure and report on our performance in managing our business and meeting our customers’ needs and use performance information to help us improve.
* Independently audit our management systems to confirm whether or not they are adequate for meeting any regulatory requirements as well as the needs of the business, our employees, our customers and others with an interest in our work.
* Use the outcomes of independent audits to help us to continuously improve and meet the needs of our customers.
* all employees and interested parties with relevant information and ensure a structured dialogue on how to improve the quality of our services.
* Regularly review the suitability and effectiveness of our systems to identify improvements that we need to make, to be more able to meet our needs and those of our customers and people who have an interest in our work.
* Develop effective relationships with our subcontractors and suppliers.

We put this policy into practice by applying policies, standards, operating procedures and processes so that we control the delivery of high-quality products and services that reliably and consistently meet our commitments to our customers.

**Objectives and strategy**

The objectives of the quality control efforts in DigiPlex are to ensure the customer feels assured and confident to undertake their day to day business without concern to the services they have purchased from us.

These objectives are achieved by raising the consciousness of quality within the corporate culture, and by establishing relevant measurements/metrics, systematic supervision and enforcement, and deviation management.

**Health and Safety**

DigiPlex is committed to making the work environment safe for its employees and others wherever we operate.  *As a minimum* DigiPlex comply with all applicable Laws and Regulations relating to health and safety in the workplace.  We inform our employees about procedures in place to protect them from generally recognized workplace hazards, using our Risk Assessment process, which ensures the wellbeing of all colleagues is not compromised and the equipment in use, is safe.  Regardless of the specific responsibility that may apply, it is the duty of every employee to co-operate in achieving compliance.  We immediately report dangerous conditions to prevent or otherwise minimize workplace accidents.  In day-to-day conditions, we integrate safety in whatever we do. To demonstrate our commitment all our data centers are certified to ISO 45001:2018

**Environmental vision**

To DigiPlex, environmental sustainability is about making responsible decisions that will reduce our business' negative impact on the environment. It is not simply about reducing the amount of waste we produce or using less energy but is concerned with developing processes that will lead to DigiPlex becoming completely sustainable in the future.  We believe Environmental Sustainability forces us to look beyond making short term gains and look at the long-term impact they are having on the natural world.

You need to consider not only the immediate impact your actions have on the environment, but the long

term implications as well. For example, when undertaking a project, you need to look at the environmental impact of the project’s entire lifecycle, from development to disposal before finalizing your designs.

As a responsible business, we are expected to lead in the area of environmental sustainability as we are considered to be the biggest contributor and are very much in a position where we can make a significant difference.

We will work in partnership with others to promote environmental care, increasing understanding of environmental issues and disseminate good practice.  DigiPlex is certified to ISO 14001:2015 at all our Data centers.

**The Quality system**

DigiPlex supports our customer's competitive quest for best value and best practice. The center is used by customers for applications ranging from disaster recovery through to frontline server space, and secure network control centers.

**Process orientation**

DigiPlex has adopted a process approach in the development and implementation of its management system for the provision of services. The aim of the management system is to enhance customer satisfaction by meeting customer requirements. In addition, each of the processes undertaken is controlled to reduce the impact of the company’s activities and services on the environment and to eliminate or minimize Health & Safety and Information Security risks to its employees and other interested parties. Continual improvement of the effectiveness and performance of the management system and processes is attained through performance measurement and the achievement of objectives.

**Management's responsibility**

It is the responsibility of the Chief Executive Officer (CEO) and his Executive Management Team (EMT) to identify the vision, direction and goals of the Company and to communicate these to staff. The EMT will lead, inspire and support their staff and promote excellence as the best way to achieve our objectives and report on progress.

The CEO oversees the development of the business plan for the Company. The plan is based on a shared understanding within the DigiPlex EMT of the critical areas of business strategy, the balance between commercial return and prudent risk-taking and the limits and boundaries beyond which risk is deemed unacceptable.

Once the business plan has been finalized, a commitment by each department is made to the achievement of the overall strategy. The business plan is regularly subjected to constructive challenge and examination to ensure it remains resilient and achievable.

To support management decisions and inform discussions with customers and other principal stakeholders, performance against strategic and operational targets is measured. The application of these performance measures provides a focus on what is important and provides the fundamentals for informed decision making.

**Resource management**

The management of people in DigiPlex is focused on the creation, development and leadership of highly engaged and competent teams linked with an integrated approach to change management. The human resource management process aims to ensure that teams have relevant and up to date skills for the work they are doing; work well together; effectively manage change and demonstrate DigiPlex’s culture and values in their dealings with customers, interested parties and with each other.

1. ***Commitment to Competence***

DigiPlex hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background skills needed to perform the job, and personal qualifications desired. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and make an appropriate hiring decision.

DigiPlex employees create individual Core Priorities that align with those of their manager, organization, and DigiPlex, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These Core Priorities are established when an employee is hired, and then updated throughout the year during one-on-one career talks with their manager. The primary focus of the career talks is to assess employee performance against their priorities and to agree on an updated list of priorities going forward.

1. ***Personnel***

DigiPlex performs employee background screening on all new recruits. DigiPlex also employs a formal performance review process to ensure employees adequately meet the responsibilities of their position, including adherence to company policies, information security policies, and workplace rules. Hiring managers may, at their discretion, initiate corrective actions, up to and including immediate termination, if any aspect of an employee's performance and conduct is not satisfactory.

**Project Management**

Project Management processes and controls define the acceptable level of quality, which is typically agreed by the customer, and describes how the project will ensure this level of quality in its deliverables and work processes. This ensures that:

* Products are built to meet agreed- upon standards and requirements
* Work processes are performed efficiently and as documented
* Non-conformances found are identified and appropriate corrective action is taken
* All work is performed safely by DigiPlex and its supply chain so that no lost time injuries occur

Project Managers liaise with relevant managers to determine customer, statutory and regulatory requirements and review these against the requirements related to the contract. The review is conducted before acceptance of an order or order amendment.

**Management review**

The CEO chairs a Management Review Meeting made up of members of the Executive Management Team as well as invited managers when required. The purpose of the meeting is to maximize the self-management of the business enabling the EMT to manage as a team, rather than just as individuals. The Company has an established auditor; their role being to ensure that the business has appropriate procedures to manage the risks to which the Company may be exposed.

**Information Security Management**

Information security requirements, policies, disaster recovery and continuity plans, and risk assessments are systematically reviewed. DigiPlex’s Information Security Management System (ISMS) is an internal management system where requirements, policies, disaster recovery and continuity plans, and risk assessments are systematically documented and updated.

**Certifications and compliance**

DigiPlex’s Management System is an integrated management system where requirements, policies, disaster recovery and continuity plans, and risk assessments are systematically documented and updated.

Policies, procedures and controls for the information security management have been designed using recognized frameworks and best practices such as ISO 27001, ISO 9001, ISO 14001, ISO 45001, ISO 23001, COBIT, ITIL and is ISO 27001, ISO 9001 ISO 14001 and ISO 45001 accredited.



.

**Regulatory compliance**

DigiPlex adhere to several regulatory and legal requirements with specific prerequisites for information security management and privacy of information and data.

**Independent security assessments**

DigiPlex collaborates with an independent security company to continuously assess and improve the operational environment from a technical security perspective and thus address staff awareness and the organization’s ability to respond to security incidents.

Independent penetration testing and vulnerability assessments of the technical infrastructure are conducted periodically (annually or more frequently).

**Whistleblowing**

There is a confidential and anonymous Whistle Blowing Hotline available for both employees and suppliers to report issues. The hotline is accessible 24x7 through email, phone, and mail. The individual may also send a letter reporting the concern to DigiPlex’s Chief HR & Compliance Officer. Employees and Suppliers are instructed that it is their duty to promptly report any concerns of suspected or known violations of the Business Code of Conduct or the Supplier Code of Practice or other DigiPlex policies or guidelines. The procedures to be followed for such a report are outlined in the Code of Business Principles and Supplier code of Practice. Employees are also encouraged to communicate the issue to their manager, their manager’s manager, of the Chief HR & Compliance Officer, or the Compliance Department.

**The components of the system used to provide the services**

1. **Infrastructure**

DigiPlex’s data center services are based on a set of requirements in terms of room/hardware rack space, UPS protection, power and physical and environmental security features. The infrastructure of the data centers are designed to ensure a secure and continuous operation in terms of redundant power systems, cooling and communication lines. Advanced systems for monitoring alarms, climate controls, power and networks are also vital elements of the systems and procedures that safeguard the physical and environmental protection of the data center.

DigiPlex’s data center have facilities that include the following physical and environmental security measures:

* Two-factor authentication for physical access
* 24/7/365 environmental monitoring (air temperature and humidity)
* Redundant cooling
* Redundant power supplies, diesel generator and UPS systems
* Redundant fiber optic internet links
* Fire detection extinguishing systems
* Leak detection systems

1. **People**

Our organization employs 80+ people, and designs, builds and operates data centers in the Nordics. We specialize in delivering best-in-class services to our customers by delivering tailored, secure and resilient environments with the highest possible availability. As a result, DigiPlex is trusted by public and private customers alike – including security sensitive organizations such as government and financial institutions.

DigiPlex’s head office is located in Oslo.

1. **Processes and procedures**

The following processes are in place and formally documented to provide data center colocation hosting Services to DigiPlex’s customers:

* Entity Level Controls
* Human Resource management
* Incident and Problem Management
* Information Security Management
* Operations management & Environmental Controls
* Physical Security and Access management
* Risk management
* Access management for customer's third-party suppliers
* Infrastructure Change Management
* Continuity Management

Descriptions of each of these are provided in the pages that follow:

**Entity Level controls**

All DigiPlex employees are accountable for understanding and adhering to the requirements contained in the DigiPlex’s Information Security Manual and any applicable supporting procedures. Individuals not employed by DigiPlex are also accountable for understanding and adhering to the requirements contained in the Information Security Policy, Manual and procedures.

**Control Objective #1:** Controls provide reasonable assurance that the management has established governance oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Entity Level Controls | CA01 | DigiPlex has established ethical values applicable to the company and its employees, supported by governing documents and commitment are communicated by management. |
| CA02 | The DigiPlex Code of Business Principles reflect a commitment to integrity and ethical business practices and regulatory compliance. They summarize the principles and policies that guide DigiPlex’s business activities and communicated to all employees via or Internet. |
| CA03 | DigiPlex has established management reporting lines with defined organization structure for governance. |
| CA04 | DigiPlex has established a formal process to communicate internal control responsibilities to all employees. |
| CA05 | DigiPlex has established a whistle blower hotline enabling anonymous and confidential communication. |
| CA06 | DigiPlex management has established a Balanced Scorecard to reflect business objectives, structure and processes. |

**Human Resources (HR)**

The management of people in DigiPlex is focused on the creation, development and leadership of highly engaged and competent teams linked with an integrated approach to change management. The human resource management process aims to ensure that teams have relevant and up to date skills for the work they are doing; work well together; effectively manage change and demonstrate DigiPlex’s culture and values in their dealings with customers, interested parties and with each other.

***Commitment to Competence***

DigiPlex hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background skills needed to perform the job, and personal qualifications desired. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and make an appropriate hiring decision.

DigiPlex employees create individual Core Priorities that align with those of their manager, organization, and DigiPlex, and are supported with customer-centric actions and measures so that everyone is working toward the same overarching vision. These Core Priorities are established when an employee is hired, and then updated throughout the year during one-on-one career talks with their manager. The primary focus of the career talks is to assess employee performance against their priorities and to agree on an updated list of priorities going forward.

***Personnel***

DigiPlex performs employee background screening on all new recruits. DigiPlex also employs a formal performance review process to ensure employees adequately meet the responsibilities of their position, including adherence to company policies, information security policies, and workplace rules. Hiring managers may, at their discretion, initiate corrective actions, up to and including immediate termination, if any aspect of an employee's performance and conduct is not satisfactory.

**Control Objective #2:** Controls provide reasonable assurance that the risk of human errors, theft, fraud or misuse of information is minimized.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Human Resource Management | CA07 | DigiPlex has defined and documented roles and responsibilities for each level within the organization structure and the same is communicated to the employees |
| CA08 | Employees are required to sign Confidentiality Agreements consisting of Non-Disclosure Agreements (NDA), and duties of insider information. |
| CA09 | Disciplinary action is taken against Associates for violating Security Policy based on disciplinary procedures documented as part of the Information security policy. |
| CA10 | Background checks are carried out for employees at the time joining as per defined company procedures. |

**Incident and problem management**

**Incident Identification**

All incidents are either submitted to DigiPlex’s ticketing management system or detected by monitoring systems. Operations focuses on identifying and resolving incidents prior to any impact on the Customer’s business. Monitoring key infrastructure components is critical for the detection of incidents.

**Incident Logging**

Incidents are logged in a ticketing management system and are managed in accordance with contractually agreed response times. All relevant information is documented.

**Incident Categorization**

All incidents are categorized. Incidents may be re categorized later in the process if deemed necessary. The Operations department utilize categorization data to facilitate for trend analysis to support its problem management process.

**Incident Prioritization**

Incidents are prioritized based on impact and severity. Level 1 & 2 incidents are escalated immediately to the Major Incident Team.

**Initial Diagnosis**

When the incident has been logged, categorized and prioritize, an attempt to diagnose the issue to fully identify the symptoms is performed. Minor Incidents (Level3) will be typical handled and solved by DigiPlex Operations without escalation or involvement of the Executive Management Team. Level 1 and 2 Incidents will be escalated to the Major Incident Team or specialized Subject Matter Experts or manufactures of the equipment.

**Major Incidents**

Major Incidents have a higher degree of business impact and urgency. They therefore require a separate management process. If the initial diagnosis identifies the incident as major, this process is triggered.

Major incidents are managed by the Executive Management Team (EMT). The EMT coordinates incident response activities, monitors development, and keeps affected parties informed on progress.

**Problem Management**

The Objective of DigiPlex’s problem management process is to ensure management of the lifecycle of all problems that happen or could happen in DigiPlex’s service deliveries. The primary objectives are to prevent problems and resulting incidents from happening, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

**Control Objective #3:** Controls provide reasonable assurance that problems and / or incidents are recorded and investigated for resolution in accordance with documented procedures.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Incident and Problem Management | CA11 | DigiPlex has established procedures for responding to security incidents and periodic evaluation of these procedures. |
| CA12 | DigiPlex has established roles and responsibilities for the design, implementation, maintenance, and execution of the incident response procedures, including the use of external resources when necessary |
| CA13 | Procedure to classify incidents as problems have been defined and documented and a root cause analysis for problems is documented. |

**Information security management**

DigiPlex has a responsibility for safeguarding internal information and IT assets. As a result, the goal for DigiPlex’s information security efforts is to minimize the risk of security breaches, downtime and loss of data through systematic and risk-based control measures. DigiPlex’s information security management is the sum of all the measures, efforts and controls that exists in order to safeguard confidentiality, integrity and availability of information assets. This includes:

* Clearly defined roles and responsibilities for information security management
* Policies, procedures, and controls based on best-practices and renowned frameworks
* Periodic risk assessments
* Automation, standardization and security technologies
* Regulatory compliance
* Independent audits and security assessments

**Roles and responsibilities**

Roles and responsibilities for the information security efforts are clearly defined:

* The CEO is ultimately responsible for the information security management, and all of DigiPlex’s information security measures and efforts.
* The information security department is responsible for implementing and ensuring compliance with DigiPlex’s information security policy, and all supplementary policies, procedures, guidelines and regulatory requirements for the management of information security
* The heads of departments and line managers are responsible for collaboration with the information security department in order to ensure compliance with the information security principles described in DigiPlex’s information security policy
* All employees are responsible for following the guidelines and principles for information security as described in DigiPlex’s information security policy, and to use the information security department as a proactive partner in information security-related matters

**Control Objective #4:** Controls provide reasonable assurance that Information Security Policies and Procedures are documented, approved, communicated, and their compliance is monitored.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Information Security Management | CA14 | DigiPlex' governing documents are documented, maintained and communicated in DigiPlex’s Information Security Management System (ISMS).  The following governing documents are revised at least annually and approved by management, and authorized by CEO or COO:  • Information Security policy statement  • Information Security Manual  • Legal register  • Business continuity policy statement  • Business continuity manual  • Crisis communication Plan  • Site business continuity plan  • Risk management, Asset risk register |

**Operations management and environmental controls**

The data center is fully monitored 24/7 by a state-of-the-art Building Management System (BMS).

The BMS gives us full control over the respective data hall environmental parameters such as temperature, humidity and power. The BMS also provides alarms on all systems to the on-duty engineers.

**Control Objective #5:** Controls provide reasonable assurance that resources are made available and monitored as per the requirements of the operations

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Operations Management and Environmental Controls | CA15 | DigiPlex has identified and manages an inventory/ overview of information assets. |
| CA16 | DigiPlex has implemented detection measures to identify anomalies that could result from failure of environmental control systems, failure of electrical/power supply, fire, and water damage. |
| CA17 | DigiPlex operations team monitors and evaluates current processing capacity and use of system components on a continuous basis. Alerts are triggered when capacity thresholds are reached and mitigating actions are initiated. |
| CA18 | Appropriate fire detection & suppression systems are in implemented at data centers.  Fire detection and suppression systems are covered under annual maintenance contract with respective vendors. |
| CA19 | Fire detection and suppression systems are maintained as per the established maintenance schedule |

**Control Objective #6:** Controls provide reasonable assurance that appropriate measures are in place to protect the data center premises and equipment from environmental hazards such as fire, excessive heating, electricity failure, water leakage, etc.

|  |  |  |
| --- | --- | --- |
| Domain | Control Activity # | Control Activity Description |
| Operations Management and Environmental Controls | CA20 | Appropriate HVAC controls are in place to maintain heat, ventilation and air conditioning in the data center. Temperature controls & monitoring is in place  HVAC systems are covered under annual maintenance contract with respective vendors. |
| CA21 | HVAC systems are maintained as per the established maintenance schedule |
| CA22 | Uninterrupted Power System (UPS) and DGs are installed at the primary and secondary data center facilities to provide uninterrupted power supply and ensure backup whenever there are any power interruptions.  UPS and DGs is covered under annual maintenance contract with respective vendors. |
| CA23 | UPS and DGs are maintained as per the established maintenance schedule |
| CA24 | Server rooms are constructed to protect server room equipment from environmental threats, e.g. overheating, power outage and excessive moisture: - Raised access floors and adequate leak detection systems - Different fire zones, the server rooms are their own fire zone |

**Physical Security and access management**

**Physical Security.**

The facilities are protected by high security perimeter fence. The risk for tailgating at the gate is avoided through the car trap with access control gates. Reception staff follow pre-defined procedures, and the cameras are used for monitoring and continuously log recording.

A man trap provides intruder protection of the data center building. Advanced security surveillance camera systems monitor both indoors and outdoors. A proximity and PIN card access system is implemented throughout.

Customer modules may optionally benefit from additional biometric access control.

**Alarm system and Security personnel**

The data centers are protected by advanced external security systems including surveillance cameras and access card readers. DigiPlex use a security firm as an “emergency responder” to any incidents at the data center sites. Security staff is operated 24/7/365, also monitoring the site grounds and car park areas of the facilities. All doors and windows at the facilities are protected with alarm systems. The data center operates a multi-layer access security system.

**Access controls**

Access is monitored through manned security presence 24/7. Security operates from a purpose-built Operations center. Security personnel, together with reception staff, operate a rigorous identification system to allow access to customers and their nominated representatives without compromising security.

Security access cards to the common areas and dedicated customer areas are only issued on receipt of written instructions from the customer’s Level 1 contact.

The data center premises have access control procedures that have been implemented in cooperation with our Customers. All new admissions must be approved by the Customer Contact. Only authorized personnel are granted access to the data center. To obtain a valid access card, a written application form must be completed and approved by the Customer Authorized Signatory.

Access is only granted using written application forms. Access cards and associated codes are personal and non-transferable. The Customer is responsible for performing quarterly entitlement reviews of personnel with access to the data center.

Visitors must be registered in the data center’s electronic visitor’s register and escorted by authorized Customer personnel. At the end of the visit, visitors are required to sign out.

**Access management for customer's third-party suppliers**

Third-party suppliers are only granted access privileges necessary for them to be able to perform specific tasks as requested by the customer. Confirmation / approval of access must always be given in writing by the Customer Contact.

**Control Objective #7:** Controls provide reasonable assurance that access to the data center premises and its assets is restricted physically and granted as per need-to-know basis

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Physical Security and Access Management | CA25 | Closed Circuit Television (CCTV) systems are installed at strategic locations at the entry and exit points of the data center facilities to record all the events.   The CCTV systems are continuously monitored by the Physical Security team.   The CCTV equipment is maintained on a regular basis. |
| CA26 | There are no windows or skylights in server rooms. All other openings (e.g. ventilation) are properly blocked or locked. |
| CA27 | The data centers are equipped with access control and alarm systems in order to detect unauthorized access to the data center premises. |
| CA28 | The access control and alarm systems are regularly maintained as per defined scheduled. |
| CA29 | DigiPlex has established and documented procedures for access creation and revocation to the data center facilities as per 'Security Manual' |
| CA30 | Access to data center facilities is revoked on the last working day of resigned/terminated employee.   Customer access is revoked based on intimation from authorized customer personnel through ticket in Service Now. |
| CA31 | DigiPlex has processes in place to periodically review physical access to ensure consistency with job responsibilities. |
| CA32 | Two factor authentication mechanism is established to access the data center. E.g. swipe card and biometric or Proximity and biometric based access control systems |
| CA33 | The data center facilities are manned by trained Security Guards round the clock, for restricting access to authorized individuals. |
| CA34 | Entry and exit details of the visitors accessing the data center facilities are logged and documented. Access to visitors is granted only after obtaining appropriate approvals from designated personnel in the management All visitors must be escorted by an authorized person while on the premises. |
| CA35 | Movements of materials within the data center is monitored and tracked, logged and only permitted with proper authorization |
| CA36 | Access to data center facilities is granted to DigiPlex employees based on approvals as per the 'access management procedures'.  Access to customers is granted based on approvals from authorized customer personnel through tickets documented in Service Now. |
| CA37 | There are formal processes for managing and controlling access to mechanical keys including: - Mechanical keys are kept in a hidden and physical secured lockbox at each location (separate systems) - Access to mechanical keys are restricted to a limited number of authorized personnel. Access to specific keys is granted based on needs - Code and fingerprint are required to gain access to lockbox |

**Risk management**

DigiPlex continuously assesses and improves its information security measures and efforts in order to reduce the risk of commercial repercussions for its customers in connection with the following security breach scenarios:

* **Confidentiality:** Unauthorized access to data due to weak information security and access management controls, cyber-attacks, theft or deliberate attack on DigiPlex’s infrastructure
* **Availability:** Unavailable systems or data caused by downtime, system failure, fire, theft and internal procedures
* **Integrity:** DigiPlex performs periodic risk assessments in order to identify and address information security risks in an operational environment that is continuously subject to development and change. The risk assessments’ results are summarized in reports with recommended actions for improvement. The reports are communicated to the information security department and upper management and used by them for prioritizing future security efforts and measures.

Control Objective #8: Controls provide reasonable assurance that the company has established a risk management framework to identify, assess, mitigate and remediate risks to the services provided to the customers and organization.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Risk Management | CA38 | DigiPlex' risk identification and assessment process includes (1) identifying information assets (physical), (2) assessing the criticality of those information assets, (3) identifying the threats to the assets (intentional, unintentional and environmental), and (4) identifying the vulnerabilities of the identified assets. |
| CA39 | Risks identified during risk assessment are documented and mitigating procedures are initiated. |

**Third Party Management**

The DigiPlex Code of Practice for Suppliers (“the Code”) defines the non-negotiable minimum standards that we ask our suppliers and their sub-tier suppliers (“the Supplier”), to respect and to adhere to when conducting business with DigiPlex. This document helps the continued implementation of our commitment to international standards such as the 10 Principles of the United Nations Global Compact, beyond our own operation. The Supplier Code of Practice reflects what expectations DigiPlex requires from outsources service providers with regard to integrity and ethical business practices

Security requirements for the subcontractors are agreed in service agreements, which include statements on the rights and obligations of both parties and a confidentiality agreement, if there is a possibility that the subcontractor personnel can see confidential information.

Control Objective #9: Controls provide reasonable assurance that system requirements, boundaries of the system, roles and responsibilities, and performance requirements are formally defined and documented with third party service providers. Compliance to service level agreements with third parties is monitored periodically by the management.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Third party management | CA40 | Security requirements for the subcontractors are agreed in service agreements, which include statements on the rights and obligations of both parties and a confidentiality agreement, if there is a possibility that the subcontractor personnel can see confidential information. |
| CA41 | The Supplier Code of Practice reflects what expectations DigiPlex requires from outsources service providers with regard to integrity and ethical business practices |

**Infrastructure change management**

Our clients depend upon us to deliver a service that provides a secure, humidity and temperature-controlled environment, with robust diverse power supplies.  Protection of the environment is therefore a key operational function. The Service Change Management process is designed to protect the service environment by ensuring that any activities that have the potential to affect that environment are risk mitigated before Approval is granted and are reviewed once completed to identify any lessons that might be learned.

Control objective #10:

Controls provide reasonable assurance that changes performed to infrastructure follow defined change management procedures to prevent unauthorized changes to the environment.

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Infrastructure Change Management | CA42 | DigiPlex has established and documented a change management process which is approved by the management.  Changes are raised, classified, tracked and approved in Service Now ticketing system. |

**Continuity management**

Dealing with a crisis is the most demanding challenge likely to face DigiPlex. The crisis may result from a fire or flood affecting the company's business continuity, a major accident or some form of business crisis. The ability to manage the crisis effectively, to handle the media issues and to restore normal operation will determine whether DigiPlex survives the experience.

**Business continuity** encompasses planning and preparation to ensure that DigiPlex can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period. As such, DigiPlex’s business continuity includes three key elements and they are

1. **Resilience**: critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions, for example through the use of redundancy and spare capacity;
2. **Recovery**: arrangements have to be made to recover or restore critical and less critical business functions that fail for some reason.
3. **Contingency:** DigiPlex has established a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

DigiPlex will respond effectively to a crisis in whatever form it might take, establishes initial procedures and defines key responsibilities for the appropriate response to business disruptions that might threaten personnel, buildings, daily operations, DigiPlex’s and customer reputation. Each Datacenter has a Site Business Continuity Plan

The principles behind this plan are:

* Risks are assessed for both probability and business impact
* Emergency Response Plans must be reasonable, practical and achievable
* Our plans can be interwoven with our customers plans

In other words, we are not planning for every possibility. Diminishing returns affect the benefits of planning for extreme cases.

Other functions of the Site Business Continuity Plan are as follows:

* Describe preventive measures that decrease the risk of a crisis event.
* Promote personal accountability and responsibility and the safe evacuation/invacuation of individuals.
* Lessen the possible impact on our operations.
* Establish procedures that can help us quickly and correctly deal with an emergency or crisis.
* Establish a process of regularly training and testing of our emergency response plans.
* Learning Lessons from every practice.

**Covid-19**

On the 5th March 2020 DigiPlex activated its Coronavirus /Pandemic Influenza – Business Continuity Plan. This plan was shared with our customers and suppliers.

For our purposes, to manage this crisis we have reviewed and refined our Company Alert state:

|  |  |
| --- | --- |
| **Alert Level - Green** | Government restrictions imposed outside of countries where DigiPlex operates  Or  Five weeks after local Government lifts all restrictions affecting local society where Digiplex operates, and DigiPlex is only experiencing minor sign of decreased resource capacity. |
| **Alert Level - Yellow** | Local Government imposes local restrictions affecting local society, including international travel not on a safe list. Local society is showing increases in number of cases and DigiPlex is beginning to have increased decreased resource capacity.  Or  Local government lifts restrictions affecting local society, including allowing international travel on a safe list, without quarantine requirements with above 75% country population with vaccinations. |
| **Alert Level - Amber** | Local Government imposes tighter local restrictions including quarantine and regular testing to enter the country. Social gatherings are restricted working from home is necessary.  Or  Local Government lifts some local restrictions affecting local society, including international travel not on a safe list, but imposes quarantine requirements. |
| **Alert Level - Red** | DigiPlex is suffering from 50% decreased resource capacity on critical staff to run any data centre.  Or  Local Government imposes strict restrictions affecting DigiPlex Operations. |

DigiPlex has operated at Alert state Yellow initially. On the 12th of March 2020 the Norwegian Government launched its Covid-19 response plan. We have been currently operating at Alert State Amber since 12th March 2020. On the 28th September 2021 , the Alert State Committee decided that it was safe to lower the Alert State from Amber to Yellow on the 4th October 2021. Then five weeks later on the 8th November , if not thing triggers our Alert State the Company will automatically lower the Alert State to Green.

Overall, although the COVID-19 pandemic has led to significant changes in the way we go about our daily lives, and has dramatically altered how we work, it has also illustrated the resilience, flexibility and positive attitude of our employees. Not only have we delivered all that we set out to in 2021, but we have, in several cases, improved processes and found better ways of working. We are a very social company, and people undoubtedly missed the in-person interactions in the office and outside of it – and we are committed to returning to this experience as soon as we can. However, morale has been kept high and engagement even increased by clever use of digital and social technologies and deep commitment to the company culture.

Last year we opened two new data centers in Norway and this year we opened another in Norway. Two additional facilitys at our Fetsund campus and a brand-new campus site in Hobøl, Holtskogen, these new facilities form part of this report.

**Control Objective #11:** Controls provide reasonable assurance that organization has documented and implemented Business Continuity plan and Disaster recovery measures in place to ensure minimal impact to operations in case of a disaster

| Domain | Control Activity # | Control Activity Description |
| --- | --- | --- |
| Continuity Management | CA43 | DigiPlex has established and documented Business Continuity and Disaster Recovery plan |
| CA44 | DigiPlex has implemented testing of the Business Continuity Plan; this is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results. |