VIETTEL IDC

Report on Viettel IDC IT Infrastructure Hosting Services System Relevant to Security, Availability, and Confidentiality.

System and Organization Control 3 (SOC 3) Report

Throughout the Period August 01, 2020, to January 31, 2021

Table of Contents

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Viettel IDC.

Scope

We have examined the Viettel IDC's (hereby Viettel) accompanying assertion titled "Viettel IDC Assertion" that the controls within Viettel IDC IT Infrastructure Hosting Services system were effective throughout the period August 01, 2020, to January 31, 2021 (description) to provide reasonable assurance that Viettel IDC service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Service Organization's Responsibilities

Viettel is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Viettel service commitments and system requirements were achieved. In Section 2, Viettel has provided the accompanying assertion titled Viettel IDC Assertion about the effectiveness of controls stated therein. When preparing its assertion, Viettel IDC is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system..

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Viettel IDC's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Viettel IDC's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Viettel IDC's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Viettel IDC's IT Infrastructure Hosting Services system were effective throughout the period August 01, 2020, to January 31, 2021, to provide reasonable assurance that Viettel IDC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Yusufali & Associates, LLC

Certified Public Accountants & IT Consultants

April 20, 2021

Viettel IDC

VIETTEL GROUP
VIETTEL – CHT COMPANY LIMITED

Viettel IDC Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Viettel IDC's IT Infrastructure Hosting Services system throughout the period August 01, 2020, to January 31, 2021, to provide reasonable assurance that Viettel IDC's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 01, 2020, to January 31, 2021, to provide reasonable assurance that Viettel IDC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2019 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Viettel IDC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 01, 2020, to January 31, 2021, to provide reasonable assurance that Viettel IDC's service commitments and system requirements were achieved based on the applicable trust services criteria.

FOR AND BEHALF OF
VIETTEL IDC, VIETNAM
Signature
Name: Le Xuan Quc
Title: Deputy Director

Viettel IDC
16th Floor, Impulse Center Building, 85 Vo Trong Phung, Thanh Xuan, Ha Noi
T: 1800 8068 | E: support@viettelidc.com.vn | W: viettelidc.com.vn

Attachment A

Note to readers: The following description of the boundaries of the system is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include everything that might be described in a description of the boundaries of the service organization's system

Viettel IDC's Description of the boundaries of the IT Infrastructure Hosting Services system

The Viettel IDC has 12 Years of formation and development, it has 5 Data Centers with international standards Rated 3 - TIA 942 covering a 25.000 m2 Floor area. Viettel IDC has 25 plus Services and Solutions and has 15.000+ Customers in several fields including 3.000+ Cloud customers.

- Data center service

  VIETTEL IDC provides data center infrastructure and IT infrastructure services: Servers, storage networks, electrical systems, air-conditioners, collocation, ... for customers to operate their IT systems.

- Cloud computing service

  VIETTEL IDC provides IT services based on cloud computing, meeting the diverse needs of computing, storage, network, security, data backup... on many deployment models: Public cloud, private cloud, hybrid cloud.

Up to now, VIETTEL IDC has 4 data centers nationwide with international standards: Rated 3 - TIA 942, meeting the diverse needs from the Government, the Bank to financial institutions, multinational companies, as well as digital service providers.

1. Phap Van-Data Center
2. Hoa Lac-Data Center
3. Hoang Hoa Tham-Data Center
4. Binh Duong-Data Center

VIETTEL IDC's data centers are built in the city center and away from the city center as well, ensuring distance for disaster prevention

- Service quality: The 4 largest and most modern Data Centers in Vietnam meeting Rated 3 - TIA 942 standard with 99.99% uptime. Diverse and confidential service ecosystem.
- Serving philosophy: Viettel's mission is to serve the Fatherland and solve problems of society and organizations, businesses. If we do not create value for customers, help customers succeed, VIETTEL IDC cannot exist for long.

VIETTEL IDC SERVICES

Colocation service means the room space, including power facilities (including UPS), air-conditioned environment, cabinet, raised floor, security control, and network provided by this center, which can provide for content provider companies, financial companies, government organizations, and enterprises that need network backup or management to store network equipment and host, except Internet System Provider (ISP). The purpose of this procedure specifies the collocation operation.

The data center will provide Colocation service includes Rack space, Domestic Shared Bandwidth, International Shared Bandwidth, Power, IP address, Switch port, Data volume.

When the customer has a requirement to use colocation service, sales staff and the Technical department will review the customer requirements and discuss with the customer if have special service requirements.

After signing the contract with the customer, sales staff will key in all relative information to OSS, including customer information, maintenance staffs, services…. Manager/Authorized person in each Datacenter will check the requisition and assign to contact window to take care of this requisition and query system owner to prepare services.

Contact window has responsibility for collecting information about service preparation from system owners and finish requisition. The next step, creating an account, sending account and customer guide document to the customer's maintenance staffs after the Manager/Authorized person verify the requisition -. When customer bring equipment in, contact windows, on-duty staff, and even system owner will handover services and help customer to install equipment

The handover will be set up in 4 copies. One is for the customer; one is for the data center and two will be sent to Sales staff. The information of customer equipment and corresponding power will be key in OSS by on-duty staff to manage

Suspension of service:

In case the customer has not paid on time or due to customer service requests, Sales staff will request suspension of that customer services on OSS

Upon receiving a request to suspend service to customers, the site manager or authorized person will handle OSS and require on-duty staff to unplug all network connection of customer's devices (under this CL) in the machine room

The suspension of customer services (when on-duty unplug customer's network connection) will be recorded on Duty System

Minus some services: When customer reduces using some service, Sales staff will create minus requisition of these services in OSS. Site managers or authorized persons in each Datacenter will check and minus the services and check customer equipment to make sure customers using services are suitable with customer's remain services on OSS. Resources of the misused services will be recovered to reuse. Next step, the site manager will create a Confirmation letter about minus services with Sales staff and the customers

Stop all services: When customers stop using the colocation service, sales staff will create one cancel requisition in OSS. The manager in each Datacenter will check and cancel all services and let the customer bring their equipment out after they pay all fees. Next step, the site manager will create a Confirmation letter about minus services with sales staff and the customers

Changing services: When the customer needs to change current using service such as Rack location, IP address, Switch port, Power (when changing equipment), the Site manager needs to check and support the customer and then create Minutes of confirmation about changing service with sales staff.

Support customer

Manage customer and equipment: When customer need to maintain equipment, on-duty staff must manage, support, and follow the Entry management procedure

Provide remote hand service: When customers need to use the remote hand service, on-duty staff will receive via the portal, fax, confirm with the customer, and implement. All actions will be recorded in the Duty system

Resolve customer complain: When the customer has comments, complaints, on-duty staff will receive, record, check and resolve (if any) and announce to the system owner and other relative units to resolve

Operation: System owner must follow procedures to manage, maintain the assigned system, On duty staff must follow SOPs and guidelines to work and support customers

COMPONENTS OF SYSTEM

The purpose of the system description is to delineate the boundaries of the system, which includes the IT Infrastructure Hosting Services outlined above, and the five system components described below: infrastructure, software, people, procedures, and data.

INTERNAL IT SYSTEM

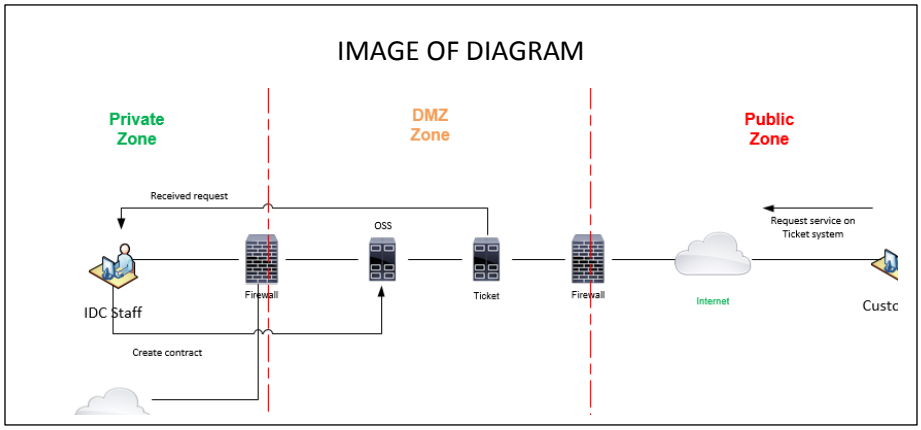
The following sections define each of the system components comprising VIETTEL IDC's colocation service and other relevant aspects of its control environment, risk assessment processes, monitoring processes, and information and communication

OVERVIEW

The internal system of Viettel IDC encompasses several systems, services, and applications that exist in three distinct environments. The three environments are:

- ZONE 1. Private Zone: containing all private systems of IDC, like AD, monitoring, backup, user computer, database,.. containing sensitive data about consumers in a hashed form. Access to the Private Zone Environment is highly restricted and requires multiple levels of approval.
- ZONE 2. DMZ Zone: contain some server of Ticket and OSS system that need to connect to the public Internet.
- ZONE 3. Public Zone: customers of IDC will connect to Ticket and OSS through this zone.

Diagram and Data Flow



The following steps outline the process by which the IDC receives, processes, and operates on Any Data. Services referenced in this section are further defined in the section called “Infrastructure and Software” below.

1. ANY Data is received from a customer in one way: via a web browser through a secure HTTPS session to the Ticket system.
2. The sales staff will analyze the request from the customer and create the environment request on the OSS system.
3. The Technical team will deploy infrastructure for customers: space, power, network. After that, they will update the status to the OSS system.
4. The sales staff will notify the customer about finishing the request.

INFRASTRUCTURE OF DATACENTER

Security gate

At the guard room, the Security Officer (guards, military soldier) controls the entrance and exit process at the gate. For the customer of Viettel IDC, the Security Department shall assist the customer to change identity card or passport to Viettel IDC's guest card via the VMS guest management system.

At the same time, Viettel IDC’s staff receives customer information from the VMS system. The Security Department also checks laptops, computers, and the devices which are brought in and out by the customer.

Network Operation Centre (NOC)

NOC is an important place in the data center. The status of all systems such as Environmental management system (temperature, humidity), security camera management system, high sensitivity smoke alarm system HSSD, fire suppression system FM200, and especially critical systems such as power systems, air-conditioning systems, and network systems, etc. are monitored in real-time and displayed on the monitor screen. The operators can detect abnormal status immediately (by observing or listening to the warning sound) and notify the system administrator to solve in the shortest possible time.

NOC staff controls access to the server room, all customers and visitors need to use Viettel IDC's guest card and exchange it for the Server room entrance card. This card only allows customers or visitors to open the door to exit the server room. Entering the Server room requires control and approval of the operational staff on duty of Viettel IDC.

All customer’s devices are recorded on the portal when the customer brings the devices to the Data center for installation. The information of the customer’s devices will be removed from the portal system when the customer takes the devices out of the Server room.

The operational staff handles requests from the customer on a 24/7 basis. Customers can send requests of services via portal, tickets, or hotline.

Infrastructure Systems

Access control system (ACS): The system is equipped with a facial recognition device (or fingerprint) in combination with the magnetic card to manage and monitor Data center access.

Early smoke detection system: The HSSD (High sensitive smoke detector) system detects and notifies of any incidents at the earliest stage, ensuring the time needed to minimize or prevent damages due to fire.

FM200 system: This system consists of probes (smoke and heat detectors), a controller, a gas tank, a piping system, and an air discharge nozzle. The system uses FM200 gas to extinguish the fire quickly and safely for humans. After the smoke detector and heat detector allow and activate the system within 30 seconds, the system will automatically release FM200 to put out the fire. At the same time, the system will automatically turn off the cold system and unlock the magnetic lock of the main door of the Server room.

Water leak detection system: This system will alert if there is water leaking from the equipment of the air conditioning system and can identify the exact location of the water leak, which helps handle problems quickly and prevent harm to the electric system.

CCTV system: The cameras are installed in the main walkways in the Server room and able to store data for 3 months. Also, operational staff on duty can supervise every location in the data center.

Environmental monitoring system (EMS): The locations of the Data center are equipped with environmental monitoring systems such as temperature, humidity, water leak detection to ensure that the environment is always within the recommended standard threshold.

Cable system

Cable trays (yellow) and UTP cable ladder (black, silver) are installed at the top of server cabinets. Network cables go in these cable trays from the Network room to server cabinets.

Cable tray: The cable tray is installed below the raised floor to avoid wave interference from the cable affecting the network signal and connection to the server cabinets.

Customer's server cabinet

Viettel IDC provides the customer with 19", 42U high rack cabinets from APC, Emerson/Vertive. A customer can rent a whole cabinet or share it with other customers.

At each server cabinet, IDC provides two power distributors, each has from 16 to 20 C13 sockets and 4 C19 sockets. Each distributor is given a different source. The power distributors in this equipment cabinet can be monitored and set warning thresholds.

Carrier Room

Carrier Room is equipped with a fiber optic system to connect from outside or from other suppliers to the location of customers located in the Data center.

Private Data center suites

For some customers who need their own rental space in the Data center, Viettel IDC can help them design, calculate and build power systems, air conditioning systems, etc.

Electric power system

The electric power system of the Data center is supplied by 02 independent medium-voltage power sources to transformers that back up each other. Also, DC is equipped with a backup generator system for electrical grid sources. In the event of power grid failure, the running time of generators ensures to work 72 hours continuously.

ATS switch cabinet system is equipped to be able to automatically switch the supply between the mains (EVN) and the Generator in the event of a power outage and vice versa. The switching time is usually from 15-30 seconds.

A Busway system is used to transmit electricity from high-voltage electricity currents, such as from an ATS cabinet system to distributed cabinets for air conditioners and UPS.

UPS system and battery system are equipped to ensure continuous electrical power for all servers and IT equipment during power outages, the minimum power saving capacity of each UPS is 15 minutes.

The STS system is equipped to enhance the safety of the electric power supply by taking 02 input power sources from 02 different UPSs to the load, the time to switch to the backup UPS power is about 2-5ms, without interrupting electric power supplies for IT equipment.

Air-conditioning system

Air-conditioning system uses precise air-conditioners to cool down from the floor, ensuring n+1 redundancy. These precise air conditioners are capable of controlling temperature and humidity conditions in the data center within the standard range.

Range: 20oC - 25oC và 40% - 60%.

SOFTWARES AND APPLICATIONS

Details of application systems used by VIETTEL IDC for delivering services to user entities

No.	Name of Application/Solution	Brief description of the Application
1	Support Ticket	Customer service support. The system receives and creates a copy of the ticket from the customer's initial request on the portal.
2	Email	Internal email system built on Open Source. The system allows sending/receiving internal emails and exchanging information with customers via email.
3	VDI	VMware Horizon provides virtual desktop to users (all employees)
4	Active Directory	Active Directory allows administrators to manage permissions and access to network resources. Active Directory stores data as objects. An object is a single element, such as a user, group, application, or device, e.g., a printer.

5	Radius	The system two-factor authentication for virtual desktop to access control for all members to access to IT system.
6	Veeam Backup and Replication	Using to backup Virtual System, internal server
7	OSS	Management of process to provide colocation service and custom component services
8	VMS	Management of customers in and out of the data center.
9	Duty	Record
10	Portal	Customer creat service request to Viettel IDC,
11	IMS	Manage system change request, system's account register, and remove
12	Property	Viettel IDC ‘s property management
13	Billing	Billing, customer's contract management
14	Anti Virus	The System anti virus for virtual desktop and desktop traditional
15	Nagios	IT System Monitoring (CPU, RAM, Services,..)
16	MRTG	IT system Monitoring (Bandwidth)
17	IPCC	IP call center
18	Syslog	Manage log of internal IT system
19	DCIM	Facility system Monitoring (UPS, STS, Generator, EMS,...)

PEOPLE

Viettel IDC Organizational Structure

Viettel IDC's organizational structure contributes to the control environment by defining key areas of responsibility and establishing appropriate lines of reporting. This organizational structure supports accountability, a prerequisite for an effective control environment. Within Viettel IDC, separate departments are established that support the Viettel IDC system.

The roles and responsibilities of each department are segregated to the extent possible. Viettel IDC has established teams with the required skills for each department. A manager heads each of these teams, with responsibility for closely supervising and reviewing the work of employees in his/her group.

The operations are under the direction of the Chief Executive Officer. VIETTEL IDC is organized into the following functional groups:

- Corporate Administration
  The CEO is responsible for overseeing strategic financial planning, legal, compliance, and corporate policy formulation. Administrative responsibilities include oversight of technology

resources and service delivery performance and ensuring that these functional areas support the strategic goals and objectives of VIETTEL IDC. The CEO also coordinates marketing and sales efforts and oversees new service offering planning.

- The Chief Technology Officer, utilizing departmental Vice Presidents and subject matter technical staff and reporting to the CEO, manages the following functions:
    - Engineering
    - Data Review
    - QA
    - Technical Operations (TechOps)

  Our Engineering department consists of software engineers, data scientists, QA engineers, and our Technical Operations Team ("TechOps"). TechOps, along with specific software engineers, are granted access permissions to administer services and systems within each of the company's three environments according to VIETTEL IDC's User Responsibility Matrix. TechOps provides account management and provisions Amazon services using automated tools such as Chef automation, Cloud Formation Templates, and Docker containers. The Engineering team manages the services, libraries, and applications deployed into the company's three environments.
- The VP of People Operations ("People Ops") is responsible for personnel management functions such as benefits, recruiting, management resources, and related company policies. People Ops supports compliance efforts through efforts such as employee training and policy enforcement.

PROCEDURES

VIETTEL IDC has documented standards, policies, and procedures to support the operation and controls over the system.

A "standard" is an enterprise-wide, mandatory directive that specifies a particular course of action. Standards support the Information Security Policy and outline a minimum baseline for policy compliance.

A "policy" is a broad statement of principles that presents management's position for each defined control area. Policies are mandatory and supported by standards, guidelines, and procedures. Policies are intended to be long-term and guide the development of rules to address specific situations.

A "procedure" is a set of detailed technical steps necessary to carry out a particular task. Procedures are often the way a policy is implemented.

Information Security Policy

Our Information Security Policy establishes the organizational information security policy for VIETTEL IDC. VIETTEL IDC is committed to managing business risk at an appropriate level and in a manner that protects VIETTEL IDC, its clients, and its clients' customers from unauthorized use or breach of private information, and protects the company's information system resources from accidental or intentional unauthorized use, modification, compromise, disclosure or destruction. Adherence to the company's Information Security Policy is mandatory and will help safeguard the security, privacy, confidentiality, and availability of sensitive information, and will protect the interests of VIETTEL IDC, its customers, personnel, and business partners.

The Security group is responsible for drafting, reviewing, updating, managing executive sign-off, and publishing the Information Security Policy. The policy is reviewed on at least an annual basis.

The comprehensive Information Security Policy includes the following sections:

- Policy Management Framework
- Roles and Responsibilities
- Acceptable Use
- Data Classification
- Data Confidentiality
- Communication Procedures
- Personal Privacy
- User Identification
- User Termination
- Systems Management
- Third-Party Access
- Encryption
- Unauthorized Duplication
- Data Backups
- Data Integrity
- Computer Systems Management
- Administrative Access control
- Network Management
- Software Management
- Employee Responsibilities
- Removable Media and Data Destruction
- External Security Reviews
- Malicious Code
- Remote Access
- Personnel Security
- Emergency Incident Reporting
- Physical and Environmental Security
- Security Awareness and Training

VIETTEL IDC Policies and Procedures

The VIETTEL IDC Information Security Policy is supplemented by many formal operating processes and procedures. These include:

- VIETTEL IDC Privacy Policy
- VIETTEL IDC Customer Data Handling Policy
- VIETTEL IDC Business Continuity Policy and Plans
- VIETTEL IDC Incident Response Policy and Plan
- VIETTEL IDC Risk Assessment Policy

- VIETTEL IDC Customer Handling Policy
- VIETTEL IDC Secure Coding Practices
- VIETTEL IDC Change Control Process
- VIETTEL IDC Configuration Management Process
- VIETTEL IDC Incident Response Process
- VIETTEL IDC Inventory Control Process
- VIETTEL IDC Administrative Access Process
- VIETTEL IDC Administrative Access Periodic Review Process
- VIETTEL IDC Secure Login Process
- VIETTEL IDC New Account Creation Process
- VIETTEL IDC User Termination Process
- VIETTEL IDC Anti-Virus Process
- VIETTEL IDC Production Systems Deployment Process
- VIETTEL IDC Systems Logging Process
- VIETTEL IDC Patch Process
- VIETTEL IDC Systems Backup Process
- VIETTEL IDC Data Retention Process
- VIETTEL IDC Media Destruction Process
- VIETTEL IDC Security Scanning Process
- VIETTEL IDC Network Device Management Process
- VIETTEL IDC Documents of operation system and handling failures.

DATA

Classification of Data

Within the context of the VIETTEL IDC has defined four levels of data classification and associated data controls. They are defined as follows:

Levels	Description	Including, but not limited to:
VIETTEL IDC Confidential Information	Information that, if disclosed, is likely to cause serious reputation and/or business damage, legal liability, or embarrassments to VIETTEL IDC, its parent company, its customers, or subscribers. This type of information requires special protection. **Data Protection** ● Confidential Information shall be protected by limiting its access to the smallest number of persons necessary for a given business function.	● Records and information relating to VIETTEL IDC and its operations ● Financial records ● Human resource records including personnel information and evaluation records ● Standards of operation ● Details about the VIETTEL IDC technology platform and infrastructure,

	● Confidential Information will not be stored on any computing device not owned or managed by VIETTEL IDC. ● Storage of Confidential Information on any device not owned and managed by VIETTEL IDC is strictly prohibited. ● Confidential Information must be stored in an encrypted format when at rest. ● Confidential Information can only be transmitted between Information Systems using secure technology protocols and never in unprotected "clear text" form. ● Confidential Information will not be shared with persons that are not Employees of the Company.	including design documents, product plans, operational standards ● Information related to customers (such as customer account information and lists of current and/or prospective customers) ● Data that gives any specific information about customers ● Passwords and cryptographic keys are used to access VIETTEL IDC Information and Information Systems.
VIETTEL IDC Customer Data	VIETTEL IDC "customer data" requires special protections that are detailed in the company's Customer Data Handling Policy. Refer to the policy for specific details.	
VIETTEL IDC Internal Information (SII)	Proprietary, non-sensitive information about the company's technology, operations, policies, procedures, etc. that, if circulated outside the company would cause little to no damage to the company's position, reputation, and/or business. Information deemed SII requires authentication to access Data Protection ● Internal Information may be stored on personal computing devices not owned or managed by VIETTEL IDC. ● Internal Information does not need to be stored in an encrypted format when at rest. ● Internal Information may be transmitted between Information Systems using insecure technology	● Policies ● Procedures ● Documents in VIETTEL IDC's internal wiki

	protocols and in unprotected "clear text" form. ● Internal Information can be shared with persons that are not Employees of the Company, assuming there is a legitimate business reason for doing so.	
VIETTEL IDC Open Information	Information that is not deemed Confidential information is deemed classified as Open Information. Open Information does not require any special protection and may be accessed by anyone. However, even though access is not restricted, VIETTEL IDC Employees are still forbidden to disclose this information to 3rd parties unless specifically authorized to do so.	

Attachment B

PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS (IN GENERAL)

Business Service	Active time	SLA of availability of service	SLA of continuity of service	
			Incidents respond time	Data recovery
Colocation	24x7	99,98%	05 minutes	N/A

Capacity of Services

1) Hoa Lac Datacenter:

- Power supply capacity: Electricity (1845 KW), UPS system (757 KW), Backup generator (2432 KW)
- The ability to provide additional seats: Rack 507
- Ability to provide transmission channels: Domestic (562 Gbps), International (37 Gbps)

2) Phap Van Datacenter:

- Power supply capacity: Grid electricity (2932 KW), UPS system (1997 KW), Backup generator (1888 KW)
- The ability to provide additional seats: 325 Rack
- Channel providing ability: Domestic (222 Gbps), International (18 Gbps)

3) Hoang Hoa Tham Datacenter:

- Power supply capacity: Electricity (5013 KW), UPS system (784 KW), Backup generator (2421 KW)
- The ability to provide additional seats: Rack 232
- Ability to provide transmission channels: Domestic (361 Gbps), International (14 Gbps)

4) Binh Duong Datacenter:

- Power supply capacity: Grid electricity (4739 KW), UPS system (1059 KW), Backup generator (3353 KW)
- The ability to provide additional seats: Rack 435

Channel providing ability: Domestic (410 Gbps), International (15 Gbps)