SHRI VILE PARLE KELAVANI MANDAL'S

INSTITUTE OF TECHNOLOGY, DHULE

NAAC Criteria Report

4.3.1 IT Infrastructure

Summary of various IT Infrastructure facilities available at SVKM's Institute of Technology, Dhule

Sr.	No. Particulars	Quantities		Pages No.
		Up To 2022-23	2023-2024	
1	Information Technology Asset Management	To all Campus	To all Campus	1
2	Cyber Security Policy	To all Campus	To all Campus	11
3	Material Transfer Request	To all Campus	To all Campus	19
4	Internet	To all Campus	To all Campus	26
5	Router	80	45	27
6	Switches	38	-	28
7	Computers	618	190	29
8	Firewall	1	-	30
9	Intrusion Detection System (IDS), Internet Provider Security (IPS)	1	-	31
10	System Software	04	-	32
11	Application Software	10	48	33
12	Smart Board	54	-	34
13	Projector	9	-	35
14	Printer	27	03	36
15	All in Printer (Xerox Machine)	3	-	37
16	Scanner	3	-	38
17	CCTV Cameras	150	125	39
18	Servers	3	-	40
19	Telecom	41	-	41
20	UPS	2	05	42
21	Laptop	1	-	43

INFORMATION TECHNOLOGY ASSET MANAGEMENT

POLICY DOCUMENT

ISSUED BY:

PREPARED BY:

Approved By:

Section	Name	Signature	Remarks
Asset Management Life Cycle			
Planning & Eligibility			
Procurement			
Deployment			
Management			
Support			
Discard & Disposal			
Reports			
Approvals			

TABLE OF CONTENTS

1. DOCUMENT SCOPE

The document covers all policies related with Management of all IT Assets.

2. STATEMENT OF POLICY

Shri Vile Parle Kelavani Mandal (SVKM) shall assess (evaluate) its IT assets for conformance to Company requirements. This policy aims to ensure that all SVKM owned IT assets are inventoried, tracked, and managed throughout each IT asset's lifecycle.

All employees and Personnel that have access to organizational IT assets must adhere to the IT asset management policy.

2.1 IT HARDWARE ASSET CONTROL

IT users, to include, employees, business partners, and contract personnel shall not remove IT assets supplied by SVKM from company premises, unless authorized to do so or specifically mentioned in their job responsibilities.

IT users are responsible for safeguarding any IT assets they remove from the company premises, including keeping these assets under their direct physical control whenever possible, and physically securing the assets (i.e. by means of lock and key) when they are not under the IT users direct physical control. The users are responsible for any damage to the asset under their possession. The recovery would happen as per HR / Finance policy.

IT users must immediately report loss or theft of any assigned IT assets to their supervisor and as appropriate, and also to IT Service Desk (ithelpdesk@nmims.edu) within 24 hours of a known occurrence.). The recovery for the lost asset is the responsibility of finance / HR. HR / department head can give the waiver on lost asset by taking necessary approvals.

IT users may use personal assets which would be governed by Institute's rules and regulations

All electronic media containing SVKM's data shall have all of that data securely removed from the electronic media before the electronic media is made surplus transferred, traded-in, otherwise disposed of, or replaced.

2.2 IT SOFTWARE ASSET CONTROL

IT users shall only use SVKM approved and appropriately licensed software on SVKM owned, leased or SVKM provided IT Assets.

Installation of software that is not approved or appropriately licensed on SVKM owned, leased, or SVKM provided IT Assets is prohibited. Strict action to be taken for any License violation reported.
Software inventory is maintained and tracked by the respective team.
On departure or asset handover the physical software license key or license is revoked under that users and added back to the software inventory.

2.3 CONFIGURATION MANAGEMENT AND CHANGE CONTROL

SVKM and its service providers are required to document IT asset configuration and changes to asset configuration at all stages of the system development life cycle.

All changes to IT assets used by SVKM shall be made in accordance with best practices as defined by the Information Technology Infrastructure Library (ITIL) framework and at a minimum include the following steps:

- Initiate change request
- Review and approve change
- Build and test change
- Create and document back up/back out plan
- Implement change
- Document change

3. INTRODUCTION & SCOPE

3.1. IT ASSET MANAGEMENT

IT Asset Management is an important business practice that involves maintaining an accurate inventory, licensing information, maintenance, and protection of hardware and software assets utilized by an organization. Understanding what IT assets are deployed at SVKM's environment will help optimize the use of IT assets throughout SVKM.

a. In accordance with the policies of SVKM, we must do what we can to gather information about our existing IT environment to better understand what we are spending on IT and how those IT investments are performing over time.

Achieving goals will provide SVKM with enhanced abilities to:

i. Make informed IT planning, procurement, investment and retirement decisions
ii. Calculate IT asset value and understand the total cost of ownership (TCO) of those assets
iii. Optimize software license usage and comply with software license requirements
iv. Manage hardware and software maintenance contracts
v. Monitor compliance with IT standards / regulations

vi. Plan for technology migration projects
vii. Allocate support resources efficiently and effectively
viii. Protect and secure IT assets
ix. Provide timely and accurate financial reports
x. Ensure that adequate warranty / AMC coverage, and business continuity and recovery plans exist based on business needs and justifications
xi. Asset management audits (preparedness, periodicity, action items)
xii. Asset management life cycles

b. The scope of IT Asset Management includes desk side computing devices like laptops, desktops, servers, Smart Boards, IP Phones and printers procured or rented by IT department. The scope also includes network devices and servers used to service the internal customer. The standard software's for day to day running of the business limited to core image and MS products and adobe acrobat writer. IT is responsible for what has been procured by IT. The ITAM is not responsible for software's and / or hardware bought for external customers / consultants and / or customer premises equipment. IT assets are categorized into the following Asset Types:
    1. Desktop workstations
    2. Laptop mobile computers
    3. Smart Boards
    4. Printers
    5. Servers for internal customers
    6. Firewalls for internal network
    7. Routers for internal network
    8. Switches for internal network
c. The roles and responsibilities for different IT assets are as per the KRA's of the respective IT managers and their teams.

4. ASSET MANAGEMENT LIFE CYCLE

The policy document, takes the following approach to handle the life cycle of the assets

i. **Planning –** defining supporting processes, setting standards for configuration and retention, aligning purchase plans to business goals, collecting aggregate information on intended purchases, and negotiating volume discounts.
ii. **Procurement –** requisitioning, approving requisitions, ordering, receiving and validating orders, tagging assets, entering asset information in a repository.
iii. **Deployment –** configuring, installing (temporary / permanent), redeployment and asset movement.
iv. **Management –** inventory/counting, monitoring usage (software tools), managing contracts for maintenance and support, and monitoring age and configuration.

v. **Support –** adding and changing configurations, repairing devices, and relocating equipment and software.
vi. **Disposition –** removing assets from service, deleting storage contents, disassembling components for reuse, terminating contracts, disposing of equipment, and removing asset from active inventory.
vii. **Reports –** reporting on all the above showcasing daily, weekly, monthly, quarterly and yearly progress on the process. Also sharing the effectiveness of the processes in place

5. PLANNING & ELIGIBILITY

Planning ensures that correct and adequate products and services are ordered keeping in mind the current / projected requirements and also the future technology trends. Eligibility of the equipment to be given is arrived at by following the asset allocation process. IT store and Local IT team conducts verification of Assets, particularly Desktops and Smart Boards and all assets with ageing > 5 years are considered for tech refresh / replacement. For rest of the categories of assets the ageing is reviewed and appropriate action is taken to continue with AMC or tech refresh.

6. PROCUREMENT

After the budget is finalized, the final AOP (annual outlay Plan) is shared by the business with the IT team. All procurement is done strictly in accordance with the Procurement Process and involves the management / commercial team.

Once asset is delivered at SVKM, the receiving department must inform ITAM of delivery of IT Assets. ITAM must verify that asset has been delivered in accordance with the Purchase Agreement. Assets need to be tagged as per company's asset-tagging policy.

7. DEPLOYMENT

The primary objective is to ensure that all assets are deployed and redeployed in a manner that optimizes their usage, while complying with legal and regulatory requirements. All assets must be tagged and tracked. The inventory registers and / or Configuration Management Database (CMDB) must be logged and updated continuously.
Deployment of assets is done only after prior approval, in adherence to the approval matrix.
Changes to the status of assets must be updated in the asset registers. This would assist in knowing number of free and deployed assets at any point of time.

There would be certain cases where the deployment of the asset has not been performed in the intended manner and it needs to be reinstalled / redeployed. Such redeployment / reinstallation must be done by personnel of the IT department only. The same must also be documented for further reference in the asset registers.

8. MANAGEMENT

For effective management of the assets, the following approach would be taken:

i. All assets will be physically inspected as per policy of the organization
ii. Monitoring would be done using software tools (SCCM, NMS tools / other vendor tools)
iii. AMC details and SLA would be maintained and tracked as per business needs
iv. Complete inventory details would be maintained up to a predefined level for each category of hardware / software as described below:
    a. For Hardware:
        i. Asset type (Desktops, Laptops, Servers, Printers, Routers and Switches).
        ii. Asset sub-type (e.g.: Printers – Inkjet, LaserJet, Impact etc.)
        iii. Asset tag
        iv. Serial number
        v. Manufacturer
        vi. Model
        vii. Vendor
        viii. Cost
        ix. Purchase / Deployment / Retirement dates
        x. Location of asset
        xi. Maintenance / warranty related information
    b. For Software:
        i. Asset sub-type (e.g.: Database, Application, Web, OS etc.)
        ii. Vendor
        iii. Vendor Product Number
        iv. Manufacturer
        v. Manufacturer Product Number
        vi. Product Name
        vii. Quantity
        viii. Version (e.g., IBM – Lotus Client – Version 8.35X)
        ix. License Agreements (e.g., EULA) or Media (eg. box for FPP)
        x. License Type
        xi. Cost
        xii. Purchase / Deployment / Retirement dates
        xiii. Location of asset
        xiv. Maintenance / warranty related information
v. Develop Competence in SAM:
    a. Conduct annual training programs for relevant stakeholders. This would be done through organized SAM workshops (2 days) conducted by software vendors or other competent bodies.

b. Ensure periodic monitoring of Proof of Licenses at document library. This is to be done in tandem with commercial / contracts team and monitoring is centralized through CMDB.
c. Identified team to conduct internal SAM reviews, to apply these skills.

9. SUPPORT

SVKM IT would support the assets that have been procured via asset management function either through in-house support or third-party vendor or a hybrid model. Support would include adding and changing configurations, repairing devices, upgrading software, and relocating equipment and software. The support would be on best effort basis for assets not procured / available in a particular location / geography, keeping the user informed of the same.

For software, support will be provided only for approved software assets. Only personnel from the IT department would be allowed to deploy / install any software assets.

10. DISCARD AND DISPOSAL

SVKM's surplus or obsolete IT assets must be discarded according to legal and environmental requirements. Therefore, all disposal procedures for retired IT assets must adhere to company-approved methods. The disposal or discard needs to comply with company's waste management policy and / or e-disposal policy.

Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

Asset discard and disposal is a special case since the asset must have sensitive data removed during or prior to discard or disposal. Below is listed the action for the device based on data sensitivity of the asset:

i. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
ii. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
iii. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
iv. High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.

The Asset discard and disposal process is to be followed for discard or disposal of assets.

11. REPORTS

To gauge the effectiveness and efficiency of the policy, certain reports will be prepared periodically:

i. Fulfillment reports
ii. SLA reports
iii. Forecasting Vs. actuals
iv. Any ad-hoc or periodic reports
v. IT asset register

vi. Asset tracker

12. APPROVALS

The policy would be approved by Management representative and Director IT and released for circulations.

13. REVIEW

This policy would be reviewed every year or as and when needed and edited. The changes would be documented in the appendices of the policy.

14. ABBREVIATIONS

IT:	Information Technology
ITAM:	IT Asset Management
SVKM:	Shri Vile Parle Kelavani Mandal
SAM:	Software Asset Management
ITIL:	Information Technology Infrastructure Library
TCO:	Total Cost of Ownership
MS:	Micro Soft
IP:	Internet Protocol
KRA:	Key Responsibility Area
AOP:	Annual Outlay Plan
CMDB:	Configuration Management Data Base
SLA:	Service Level Agreement
CIO:	Chief Information Officer
NMS:	Network Monitoring System
BYOD:	Bring Your Own Device
AMC:	Annual Maintenance Contract
SCCM:	System Center Configuration Manager

Cyber Security Policy

Version Control & Change History

Ver	Date	Section	Amendment / Change	Action	by
1.0	31 Jul 2023	Initial Draft	Basic Schema & details	Created	CISO
				Reviewed	IT Director
				Approved	
				Maintained	CISO
1.1	31 Aug 2023	Security Measures & Actions	Actual action taken for each measure are added	Created	CISO
	31 Aug 2023			Reviewed	IT Director
	02 Nov 2023			Approved	Executive & Managing Committee Member
				Maintained	CISO

1. Purpose

This cybersecurity policy aims to provide guidelines, principles and procedures to ensure the confidentiality, integrity and availability of the information systems, data and assets belonging to the Public Charitable Trust “Shri Vile Parle Kelavani Mandal (SVKM)”, the Deemed University “Narsee Monjee Institute of Management Studies (NMIMS)”, its affiliated educational institutions and its stakeholders. The purpose of this policy is to protect sensitive information, maintain privacy of personal data and mitigate cybersecurity risks.

2. Scope

This policy is applicable to all staff members (teaching, non-teaching, and third parties), students, independent contractors, suppliers, partners, and anybody else who has access to SVKM & NMIMS's networks, data, or information systems. It includes any hardware, software, and networks that the SVKM & NMIMS own, use, implement, or control.

3. Roles and Responsibilities

3.1. OB & Senior Management: OB & Senior management is in charge of developing the organization's overall cybersecurity strategy, allocating the necessary funds, and fostering a climate of security awareness among all employees.

3.2. IT & Security Department: The IT & Security departments are in charge of implementing and maintaining technical security controls, keeping an eye on systems, performing risk analyses, controlling access privileges, and responding to security incidents.

3.3. Employees (teaching, non-teaching) and students: All employees and students have a duty to abide by this policy, report security events, and take part in cybersecurity awareness and training programs.

4. Information Classification and Handling

4.1. Data Classification: Information assets should be classified into categories based on their sensitivity and criticality. A classification scheme should be established, clearly defining the handling and protection requirements for each category, in line with relevant regulations and privacy laws.

4.2. Data Protection: Personal data should be collected, processed, stored, and shared in compliance with applicable privacy laws. Consent should be obtained when required,

and appropriate security measures should be implemented to protect personal data from unauthorized access or disclosure.

4.3. Data Access and Handling: Access to information should be granted on a need-to-know and least privilege basis. Employees and students should be educated on their responsibilities for protecting information, including data handling procedures, data storage, transmission, and disposal practices.

4.4. Data Retention and Disposal: A data retention policy should be established to determine the duration for which information should be retained based on legal, regulatory, and business requirements. Secure disposal methods should be implemented for information and storage media that are no longer needed.

5. Security Measures & Actions

5.1. Access Control: Access to information systems, networks, and data should be granted based on job roles and responsibilities, utilizing the principle of least privilege. User accounts should be managed securely, with strong password policies, multi-factor authentication where possible, and regular access reviews.

Access are granted based on job roles and responsibilities, such as Students, Staff and Faculty. Regular access reviews are conducted every year. We are using “Captive Portal” for user to browse the Internet and that facilitates the management of access by users in the wireless network.

5.2. Network Security: Firewalls, intrusion detection and prevention systems, and secure network configurations should be implemented to protect against unauthorized access, external threats, and network vulnerabilities.

We use FortiGate NGFWs firewalls in our Network Infrastructure, The Unified Threat Protection (UTP) and the Enterprise bundles licenses which includes the FortiGuard services such as FortiCare Support , Firmware & General Updates, Intrusion Prevention, Antivirus, Web & Email Filtering , SDWAN and Cloud Sandbox .It gives us comprehensive protection against known and unknown threats (e.g., ransomware, malicious botnets, zero-day, and encrypted malware). Firewalls policies are reviewed with regular interval. Network Security Devices are hardened for Best Security Configurations and updated time to time for Security Patch

5.3. Network Segmentation: Network segmentation should be implemented to divide the organization's network into separate segments, based on security requirements, and to

restrict lateral movement within the network. This helps contain potential breaches and limit the impact of security incidents.

We have done Network segmentation with VLANs and created isolated networks within the data center. Each network is having separate broadcast domain.

5.4. Web Application Firewall (WAF): A Web Application Firewall (WAF) shall be implemented to protect web applications and websites from common security threats, such as SQL injection, cross-site scripting (XSS), and other application-layer attacks. The WAF should be configured to provide continuous monitoring, detection, and mitigation of web-based threats, and regular updates and maintenance of the WAF should be conducted to ensure optimal security posture.

We are using Fortiweb as Web application firewall (WAF) appliance which can detect and block known web application attacks. We have configured WAF profiles to use signatures and constraints to examine web traffic and also enforced an HTTP method policy, which controls the HTTP method that matches the specified pattern.

5.5. Endpoint & Malware Protection: All devices and systems should have up-to-date antivirus software, malware protection, and regular scanning and updates to prevent and detect malware infections.

We are using Symantec Endpoint Protection software suite which provide us comprehensive endpoint security and protection. The suite includes advanced malware protection, application control, exploit prevention. We ensure that all detections are mitigated, cleaned and reported. We ensure to have latest update of Virus signatures.

5.6. Email Security: Email security measures shall be implemented to protect against phishing attacks, malware distribution, and unauthorized disclosure of sensitive information by using email filtering systems, implementing anti-spam and anti-phishing controls.

We are using Microsoft o365 cloud services as an email service including Spam Email Filter. All the spams with critical level are handled by Administrator.

5.7. Data Encryption: Encryption should be used for sensitive data at rest and in transit, especially when stored on portable devices or transmitted over public networks.

We have implemented all our communication between Applications over Internet by HTTPS and TLS 1.1 minimum. User data is encrypted internally as well while communicating with Intra applications.

5.8. Incident Response: An incident response plan should be developed and maintained, including procedures for detecting, reporting, and responding to security incidents. This should encompass steps for containment, investigation, mitigation, and recovery.

We have communicated process and dedicated email id through which Incidents are reported to IR team by all stakeholders. Incident Response team then perform Investigation and Root Cause Analysis (RCA) and different Mitigation, Containment and Remediation applicable case to case are done and recorded for future references.

5.9. Security Monitoring: Continuous monitoring of information systems, networks, and data should be conducted to detect and respond to potential security incidents and vulnerabilities.

We are using FortiAnalyzer which is having 30 days log retention, analytics, and reporting. We have enforced security rules on firewalls to monitor and filter incoming and outgoing traffic. We are manually monitoring security threats and proactively work on events alerts emails generated by Security devices.

5.10. Security Testing: Regular security testing, including vulnerability assessments, penetration testing, and security audits, should be performed to identify and address vulnerabilities and weaknesses in systems and applications.

We perform Security Audits (VAPT) by Third Party experts for network infrastructure, applications (Web, Mobile), SAP. These audits are Black box and Grey box in nature. We follow up with stakeholders for mitigation of the findings and outcome of these audits. As of today there is zero Critical vulnerability exist in our infrastructure. We share dashboards with stakeholders for visibility on security posture.

5.11. Patch Management and Security Updates: An effective patch management process shall be implemented to ensure that operating systems, software applications, and firmware are kept up to date with the latest security patches and updates. This includes establishing a patch management schedule, testing patches before deployment, and promptly applying critical security patches. Regular monitoring and reporting on patch compliance should be conducted to mitigate the risk of known vulnerabilities being exploited.

We perform regular security patch management to ensure our servers, software and applications are up-to-date and pose no lateral threat. We perform patch management by combination of automatic and manual as and when necessary for assets that are susceptible to cyberattacks, helping us to reduce overall security risk.

5.12. Printing Security: Printing activity should be Secure and access should be provided to authorized users. Sensitive Data printing activity should be monitored for data leakage and disposal of any expired document containing sensitive data should be carried out by respective department heads to avoid dumpster diving.

We are using HP Secure Managed Print Services that adds extra layers of security. Print sensitive documents to shared printers without security worries and reduce waste from accidental and forgotten print.

5.13. Physical Security: Physical access controls, such as restricted access to data centers, server rooms, and storage facilities, should be implemented to safeguard critical infrastructure and assets.

We have at each campus and locations implemented security cameras and access control gates operated by smart cards with biometrics such as face and thumb impression. Control Centers are monitored by Security personnel 24by7.

6. Security Awareness and Training

Regular security awareness and training programs should be conducted for employees, students, and other stakeholders to promote a culture of cybersecurity. This should include educating them about threats, best practices, policies, and procedures related to information security.

We take following actions for training and awareness:

1) Regularly organize training for staff on cybersecurity best practices & Awareness.

2) Publish and communicate Cyber Security Newsletters every month to all staff.

3) Sharing information time to time on Global security incidence/Zero day/Vulnerability, etc. with all Staff.

7. Compliance and Audit

Periodic security audits, vulnerability assessments, and risk assessments of Network, Applications, Data & IT Assets should be conducted to evaluate the effectiveness of security controls, identify vulnerabilities, and ensure compliance with relevant laws, regulations, and industry standards.

We perform security audits, vulnerability assessments, and risk assessments of Network, Applications, Data & IT Assets by third part experts. We share compliance details with regulatory bodies in India time to time.

8. Policy Review and Revision

This cybersecurity policy should be reviewed and updated periodically to reflect changes in technology, evolving threats, regulatory requirements, and organizational needs. Reviews should involve key stakeholders and incorporate lessons learned from security incidents and audits.

9.Policy Acceptance

By joining SVKM, NMIMS and their affiliated educational institutions as an employee or student, individuals acknowledge their understanding of and agreement to comply with this cybersecurity policy and its associated procedures.

Shri Vile Parle Kelavani Mandal

Bhaidas Sabhagriha Bldg., 2nd floor,

Bhakti Vedanta Swami Marg,

Vile Parle (West), Mumbai - 400 056

Material Transfer Request Form

Initiated as per Instruction from Mr. Deepak Gursahani Sir- Director-IT

Organization Details:

From (Institute Name): - **SVKM IOT .**

To (Institute Name): - Shri Bhandari Sir (SES, Shirpur)

Company Code: -

Company Code: -

Plant code: -

Plant code: -

Asset no. / Material no. (P.O. No.): -

Qty: - **165 no's OLD AIO Desktops.**

Material Description: - Excel is Attached.

Value of Goods in Rs. .....

Recipient Asset/ Non-Asset transfer document no. and date

Initiated by: -

Amol Sonawane

Approved by: -

Mr. Bhushan Kulkarni

IT – Jt. Director.

@ Rs 1500/-

09157202

Shri Jagat Killawala
Executive & Managing Cmt. Member
Shri Vile Parle Kelavani Mandal

Shri Vile Parle Kelavani Mandal

Bhaidas Sabhagriha Bldg., 2nd floor,

Bhakti Vedanta Swami Marg,

Vile Parle (West), Mumbai - 400 056

Material Transfer Request Form

Initiated as per Instruction from Mr. Deepak Gursahani Sir- Director-IT

Organization Details:	
From (Institute Name): - **SVKM IOT .**	To (Institute Name): - Shri Bhandari Sir (SES, Shirpur)
Company Code: -	Company Code: -
Plant code: -	Plant code: -
Asset no. / Material no. (P.O. No.): -	
Qty: - **165 no's OLD AIO Desktops.**	
Material Description: - Excel is Attached.	
Value of Goods in Rs.	

Recipient Asset/ Non-Asset transfer document no. and date

Initiated by: -

Amol Sonawane

Approved by: -

Mr. Bhushan Kulkarni

IT – Jt. Director.

Shri Vile Parle Kelavani Mandal

Bhaidas Sabhagriha Bldg., 2nd floor,

Bhakti Vedanta Swami Marg,

Vile Parle (West), Mumbai - 400 056

Sr. No.	Serial No. of Desktop	Asset No.	Make & Model	Purchase Year	working Status
1	8CC8360J0Y	19000077 0000	HP 200 G3 All-in-One PC	2018	Working
2	8CC8360J2P	19000078 0000	HP 200 G3 All-in-One PC	2018	Working
3	8CC8360J0G	19000079 0000	HP 200 G3 All-in-One PC	2018	Working
4	8CC8360HZD	19000080 0000	HP 200 G3 All-in-One PC	2018	Working
5	8CC8360J0S	19000081 0000	HP 200 G3 All-in-One PC	2018	Working
6	8CC8360J0Z	19000082 0000	HP 200 G3 All-in-One PC	2018	Working
7	8CC8360J12	19000083 0000	HP 200 G3 All-in-One PC	2018	Working
8	8CC8360HZC	19000084 0000	HP 200 G3 All-in-One PC	2018	Working
9	8CC8360J16	19000085 0000	HP 200 G3 All-in-One PC	2018	Working
10	8CC8360J04	19000086 0000	HP 200 G3 All-in-One PC	2018	Working
11	8CC8360J1S	19000087 0000	HP 200 G3 All-in-One PC	2018	Working
12	8CC8360J1H	19000088 0000	HP 200 G3 All-in-One PC	2018	Working
13	8CC8360HZQ	19000089 0000	HP 200 G3 All-in-One PC	2018	Working
14	8CC8360J17	19000090 0000	HP 200 G3 All-in-One PC	2018	Working
15	8CC8360J0B	19000091 0000	HP 200 G3 All-in-One PC	2018	Working
16	8CC8360J2J	19000092 0000	HP 200 G3 All-in-One PC	2018	Working
17	8CC8360HZH	19000093 0000	HP 200 G3 All-in-One PC	2018	Working
18	8CC8360HZN	19000094 0000	HP 200 G3 All-in-One PC	2018	Working
19	8CC8360J03	19000095 0000	HP 200 G3 All-in-One PC	2018	Working
20	8CC8360J0L	19000096 0000	HP 200 G3 All-in-One PC	2018	Working
21	8CC8360HZ8	19000097 0000	HP 200 G3 All-in-One PC	2018	Working
22	8CC8360J2K	19000098 0000	HP 200 G3 All-in-One PC	2018	Working
23	8CC8360J01	19000099 0000	HP 200 G3 All-in-One PC	2018	Working
24	8CC8360J14	19000100 0000	HP 200 G3 All-in-One PC	2018	Working
25	8CC8360J22	19000101 0000	HP 200 G3 All-in-One PC	2018	Working
26	8CC8360J11	19000002 0000	HP 200 G3 All-in-One PC	2018	Working
27	8CC8360J18	19000003 0000	HP 200 G3 All-in-One PC	2018	Working
28	8CC8360J0N	19000004 0000	HP 200 G3 All-in-One PC	2018	Working
29	8CC8360J1N	19000005 0000	HP 200 G3 All-in-One PC	2018	Working
30	8CC8360J2M	19000006 0000	HP 200 G3 All-in-One PC	2018	Working
31	8CC8360J0Q	19000007 0000	HP 200 G3 All-in-One PC	2018	Working
32	8CC8360J1T	19000008 0000	HP 200 G3 All-in-One PC	2018	Working
33	8CC8360J36	19000009 0000	HP 200 G3 All-in-One PC	2018	Working
34	8CC8360HZW	19000010 0000	HP 200 G3 All-in-One PC	2018	Working
35	8CC8360J1P	19000011 0000	HP 200 G3 All-in-One PC	2018	Working

36	8CC8360J13	19000012 0000	HP 200 G3 All-in-One PC	2018	Working
37	8CC8360J02	19000013 0000	HP 200 G3 All-in-One PC	2018	Working
38	8CC8360J0R	19000014 0000	HP 200 G3 All-in-One PC	2018	Working
39	8CC8360J31	19000015 0000	HP 200 G3 All-in-One PC	2018	Working
40	8CC8360J0T	19000016 0000	HP 200 G3 All-in-One PC	2018	Working
41	8CC8360J1L	19000017 0000	HP 200 G3 All-in-One PC	2018	Working
42	8CC8360HZZ	19000018 0000	HP 200 G3 All-in-One PC	2018	Working
43	8CC8360J1J	19000019 0000	HP 200 G3 All-in-One PC	2018	Working
44	8CC8360HZL	19000020 0000	HP 200 G3 All-in-One PC	2018	Working
45	8CC8360J0J	19000021 0000	HP 200 G3 All-in-One PC	2018	Working
46	8CC8360J33	19000022 0000	HP 200 G3 All-in-One PC	2018	Working
47	8CC8360J1M	19000023 0000	HP 200 G3 All-in-One PC	2018	Working
48	8CC8360J09	19000024 0000	HP 200 G3 All-in-One PC	2018	Working
49	8CC8360J1K	19000025 0000	HP 200 G3 All-in-One PC	2018	Working
50	8CC8360J2D	19000026 0000	HP 200 G3 All-in-One PC	2018	Working
51	8CC8360J0W	19000027 0000	HP 200 G3 All-in-One PC	2018	Working
52	8CC8360J34	19000028 0000	HP 200 G3 All-in-One PC	2018	Working
53	8CC8360J1X	19000029 0000	HP 200 G3 All-in-One PC	2018	Working
54	8CC8360J00	19000030 0000	HP 200 G3 All-in-One PC	2018	Working
55	8CC8360J2Z	19000031 0000	HP 200 G3 All-in-One PC	2018	Working
56	8CC8360J25	19000032 0000	HP 200 G3 All-in-One PC	2018	Working
57	8CC8360J19	19000033 0000	HP 200 G3 All-in-One PC	2018	Working
58	8CC8360J23	19000034 0000	HP 200 G3 All-in-One PC	2018	Working
59	8CC8360J2R	19000035 0000	HP 200 G3 All-in-One PC	2018	Working
60	8CC8360J2N	19000036 0000	HP 200 G3 All-in-One PC	2018	Working
61	8CC8360J1D	19000037 0000	HP 200 G3 All-in-One PC	2018	Working
62	8CC8360J3D	19000038 0000	HP 200 G3 All-in-One PC	2018	Working
63	8CC8360J39	19000039 0000	HP 200 G3 All-in-One PC	2018	Working
64	8CC8360J2B	19000040 0000	HP 200 G3 All-in-One PC	2018	Working
65	8CC8360J2W	19000041 0000	HP 200 G3 All-in-One PC	2018	Working
66	8CC8360J2X	19000042 0000	HP 200 G3 All-in-One PC	2018	Working
67	8CC8360J06	19000043 0000	HP 200 G3 All-in-One PC	2018	Working
68	8CC8360J0V	19000044 0000	HP 200 G3 All-in-One PC	2018	Working
69	8CC8360J1V	19000045 0000	HP 200 G3 All-in-One PC	2018	Working
70	8CC8360HZP	19000046 0000	HP 200 G3 All-in-One PC	2018	Working
71	8CC8360HZG	19000047 0000	HP 200 G3 All-in-One PC	2018	Working
72	8CC8360J3C	19000048 0000	HP 200 G3 All-in-One PC	2018	Working

Shri Vile Parle Kelavani Mandal

Bhaidas Sabhagriha Bldg., 2nd floor,

Bhakti Vedanta Swami Marg,

Vile Parle (West), Mumbai - 400 056

73	8CC8360HZV	19000049 0000	HP 200 G3 All-in-One PC	2018	Working
74	8CC8360HZF	19000050 0000	HP 200 G3 All-in-One PC	2018	Working
75	8CC8360J1W	19000051 0000	HP 200 G3 All-in-One PC	2018	Working
76	8CC8360HZJ	19000052 0000	HP 200 G3 All-in-One PC	2018	NOT WORKING (Adapter is not Available)
77	8CC8360HZK	19000053 0000	HP 200 G3 All-in-One PC	2018	Working
78	8CC8360HZY	19000054 0000	HP 200 G3 All-in-One PC	2018	Working
79	8CC8360J2L	19000055 0000	HP 200 G3 All-in-One PC	2018	Working
80	8CC8360J10	19000056 0000	HP 200 G3 All-in-One PC	2018	Working
81	8CC8360J15	19000057 0000	HP 200 G3 All-in-One PC	2018	Working
82	8CC8360J0F	19000058 0000	HP 200 G3 All-in-One PC	2018	Working
83	8CC8360J2F	19000059 0000	HP 200 G3 All-in-One PC	2018	Working
84	8CC8360J24	19000060 0000	HP 200 G3 All-in-One PC	2018	Working
85	8CC8360J0D	19000061 0000	HP 200 G3 All-in-One PC	2018	Working
86	8CC8360J0M	19000062 0000	HP 200 G3 All-in-One PC	2018	Working
87	8CC8360J2H	19000063 0000	HP 200 G3 All-in-One PC	2018	Working
88	8CC8360J0H	19000064 0000	HP 200 G3 All-in-One PC	2018	Working
89	8CC8360J2C	19000065 0000	HP 200 G3 All-in-One PC	2018	Working
90	8CC8360J1G	19000066 0000	HP 200 G3 All-in-One PC	2018	Working
91	8CC8360J0K	19000067 0000	HP 200 G3 All-in-One PC	2018	Working
92	8CC8360J1B	19000068 0000	HP 200 G3 All-in-One PC	2018	Working
93	8CC8360J1C	19000069 0000	HP 200 G3 All-in-One PC	2018	Working
94	8CC8360HZX	19000070 0000	HP 200 G3 All-in-One PC	2018	Working
95	8CC8360J07	19000071 0000	HP 200 G3 All-in-One PC	2018	Working
96	8CC8360HZ7	19000072 0000	HP 200 G3 All-in-One PC	2018	Working
97	8CC8360HZS	19000073 0000	HP 200 G3 All-in-One PC	2018	Working
98	8CC8360HZB	19000074 0000	HP 200 G3 All-in-One PC	2018	Working
99	8CC90432D5	19000075 0000	HP 200 G3 All-in-One PC	2018	Working
100	8CC8360J0C	19000076 0000	HP 200 G3 All-in-One PC	2019	Working
101	8CC9260K07	19000159 0000	HP 200 G3 All-in-One PC	2019	Working
102	8CC9260JZN	19000160 0000	HP 200 G3 All-in-One PC	2019	Working
103	8CC9260JZV	19000161 0000	HP 200 G3 All-in-One PC	2019	Working
104	8CC9260JZQ	19000162 0000	HP 200 G3 All-in-One PC	2019	Working
105	8CC9260K17	19000163 0000	HP 200 G3 All-in-One PC	2019	Working
106	8CC9260JYD	19000164 0000	HP 200 G3 All-in-One PC	2019	Working

107	8CC9260K0L	19000165 0000	HP 200 G3 All-in-One PC	2019	Working
108	8CC9260K0Q	19000166 0000	HP 200 G3 All-in-One PC	2019	Working
109	8CC9260K0C	19000167 0000	HP 200 G3 All-in-One PC	2019	Working
110	8CC9260JYN	19000168 0000	HP 200 G3 All-in-One PC	2019	Working
111	8CC9260JZF	19000169 0000	HP 200 G3 All-in-One PC	2019	Working
112	8CC9260K12	19000170 0000	HP 200 G3 All-in-One PC	2019	Working
113	8CC9260K0S	19000171 0000	HP 200 G3 All-in-One PC	2019	Working
114	8CC9260JZ7	19000172 0000	HP 200 G3 All-in-One PC	2019	Working
115	8CC9260JZ3	19000173 0000	HP 200 G3 All-in-One PC	2019	Working
116	8CC9260JZ0	19000174 0000	HP 200 G3 All-in-One PC	2019	Working
117	8CC9260JZM	19000175 0000	HP 200 G3 All-in-One PC	2019	Working
118	8CC9260JZS	19000176 0000	HP 200 G3 All-in-One PC	2019	Working
119	8CC9260JYX	19000177 0000	HP 200 G3 All-in-One PC	2019	Working
120	8CC9260JYM	19000178 0000	HP 200 G3 All-in-One PC	2019	Working
121	8CC9260K19	19000180 0000	HP 200 G3 All-in-One PC	2019	Working
122	8CC9260JZB	19000181 0000	HP 200 G3 All-in-One PC	2019	Working
123	8CC9260K08	19000182 0000	HP 200 G3 All-in-One PC	2019	Working
124	8CC9260K16	19000138 0000	HP 200 G3 All-in-One PC	2019	Working
125	8CC9260JZP	19000139 0000	HP 200 G3 All-in-One PC	2019	Working
126	8CC9260JYK	19000140 0000	HP 200 G3 All-in-One PC	2019	Working
127	8CC9260JZ6	19000141 0000	HP 200 G3 All-in-One PC	2019	Working
128	8CC9260K01	19000142 0000	HP 200 G3 All-in-One PC	2019	Working
129	8CC9260K1B	19000143 0000	HP 200 G3 All-in-One PC	2019	Working
130	8CC9260K13	19000144 0000	HP 200 G3 All-in-One PC	2019	Working
131	8CC9260JZ2	19000145 0000	HP 200 G3 All-in-One PC	2019	Working
132	8CC9260K0F	19000146 0000	HP 200 G3 All-in-One PC	2019	Working
133	8CC9260K15	19000147 0000	HP 200 G3 All-in-One PC	2019	Working
134	8CC9260JZH	19000148 0000	HP 200 G3 All-in-One PC	2019	Working
135	8CC9260JZ9	19000149 0000	HP 200 G3 All-in-One PC	2019	Working
136	8CC9260JYW	19000150 0000	HP 200 G3 All-in-One PC	2019	Working
137	8CC9260K0Z	19000151 0000	HP 200 G3 All-in-One PC	2019	Working
138	8CC9260JZK	19000152 0000	HP 200 G3 All-in-One PC	2019	Working
139	8CC9260JYB	19000153 0000	HP 200 G3 All-in-One PC	2019	Working
140	8CC9260JZR	19000154 0000	HP 200 G3 All-in-One PC	2019	Working
141	8CC9260JZW	19000155 0000	HP 200 G3 All-in-One PC	2019	Working
142	8CC9260JY4	19000156 0000	HP 200 G3 All-in-One PC	2019	Working
143	8CC9260JYZ	19000157 0000	HP 200 G3 All-in-One PC	2019	Working

144	8CC9260JY6	19000158 0000	HP 200 G3 All-in-One PC	2019	Working
145	8CC9260K00	19000118 0000	HP 200 G3 All-in-One PC	2019	Working
146	8CC9260K0B	19000119 0000	HP 200 G3 All-in-One PC	2019	Working
147	8CC9260K14	19000120 0000	HP 200 G3 All-in-One PC	2019	Working
148	8CC9260K02	19000121 0000	HP 200 G3 All-in-One PC	2019	Working
149	8CC9260K05	19000122 0000	HP 200 G3 All-in-One PC	2019	Working
150	8CC9260JZY	19000123 0000	HP 200 G3 All-in-One PC	2019	Working
151	8CC9260JYQ	19000124 0000	HP 200 G3 All-in-One PC	2019	Working
152	8CC9260K0W	19000125 0000	HP 200 G3 All-in-One PC	2019	Working
153	8CC9260JYS	19000126 0000	HP 200 G3 All-in-One PC	2019	Working
154	8CC9260JYR	19000127 0000	HP 200 G3 All-in-One PC	2019	Working
155	8CC9260JZT	19000128 0000	HP 200 G3 All-in-One PC	2019	Working
156	8CC9260K0D	19000129 0000	HP 200 G3 All-in-One PC	2019	Working
157	8CC9260K0X	19000130 0000	HP 200 G3 All-in-One PC	2019	Working
158	8CC9260JYG	19000131 0000	HP 200 G3 All-in-One PC	2019	Working
159	8CC9260K1C	19000132 0000	HP 200 G3 All-in-One PC	2019	Working
160	8CC9260K03	19000133 0000	HP 200 G3 All-in-One PC	2019	Working
161	8CC9260K0H	19000134 0000	HP 200 G3 All-in-One PC	2019	Working
162	8CC9260JZ4	19000135 0000	HP 200 G3 All-in-One PC	2019	Working
163	8CC9260JZD	19000136 0000	HP 200 G3 All-in-One PC	2019	Working
164	8CC9260K0N	19000137 0000	HP 200 G3 All-in-One PC	2019	Working
165	8CC9260JYL	19000179 0000	HP 200 G3 All-in-One PC	2019	Working

1. Internet

Sr. No	Configuration	Quantities	Year of purchasing
01	Bharat Sanchar Nigam Limited(34 MBPS)	To all Campus	24/02/2017
02	INTERNET LEASE LINE (200MBPS)	To all Campus	15/12/2019
03	Bharat Sanchar Nigam Limited(40MBPS)	To all Campus	2022
04	INTERNET LEASE LINE (350MBPS)	To all Campus	08/03/2023

Infinite Broadnet Solution Pvt Ltd
29,"Yashodhan Colony" Walwadi Shivar , DHULE-424001
Mb:9764441644

Invoice

Infinite Broadnet Soution Pvt Ltd 29,"Yashodhan Colony" Walwadi Shivar , DHULE-424001 **Company's PAN : AADCI8694Q** **GST No. : 27AADCI8694Q1ZI** **SAC Code: 998422**	**Invoice No.- SVKM01** Invoice Date-08 March 2023 State :MH Code:27
Buyer Shri Vile Parle Kelavani Mandal's Institute Of Technology, Survey No. 499, Plot No 02, Behind Gurudwara, Mumbai Agra National Highway, Dhule -424 001, Maharashtra, India	Destination – Dhule

Sr.No	Description	Rate	Quantity	Amount
1	INTERNET LEASE LINE 350MBPS Billing period: 05/03/2023 to 04/06/2023			174999
	Total Amount Before Tax:			**174999.00**
	Add:CGST@9%			**15749.91**
	Add:SGST@9%			**15749.91**
	Total Amount After Tax:			**206498.82**

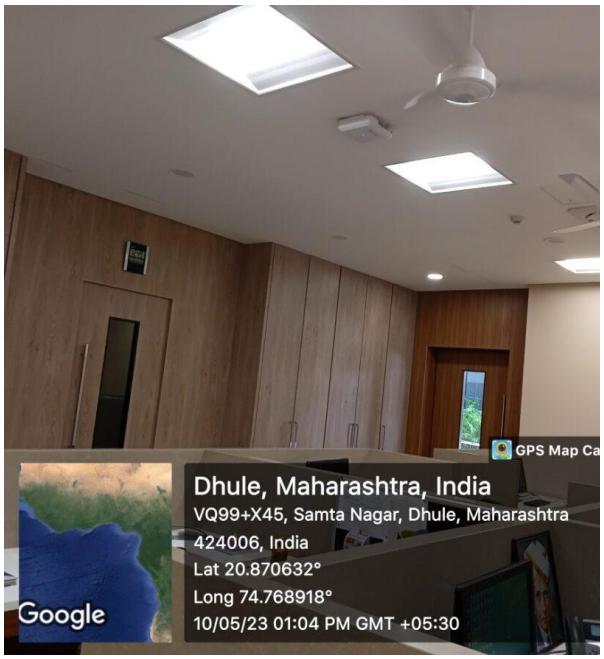
In words : Two Lac Six thousand Four Hundred Ninty Eight and Eighty Two paise

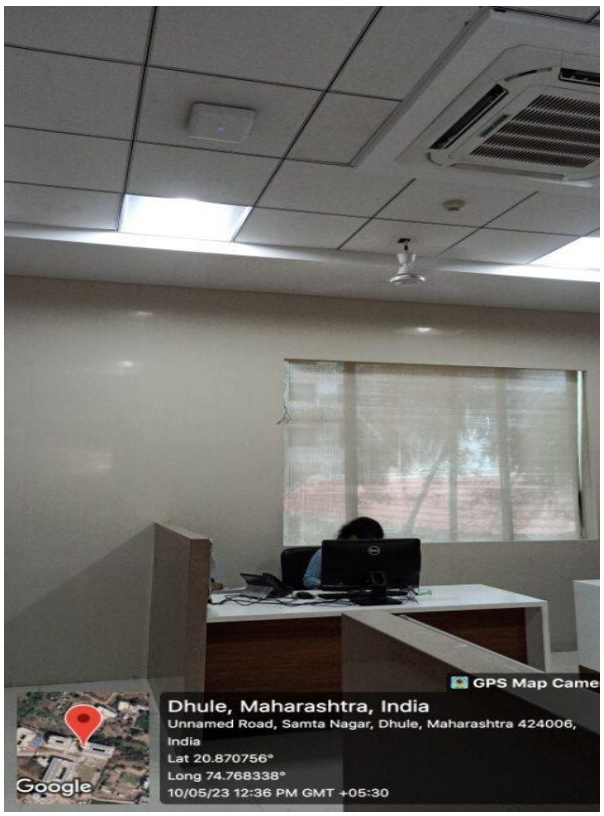
Account Details :
Account Name: Infinite Broadnet Solution Pvt Ltd
Account No : 646305004347
IFSC code: ICIC0006463
Bank : ICICI Bank , Dhule

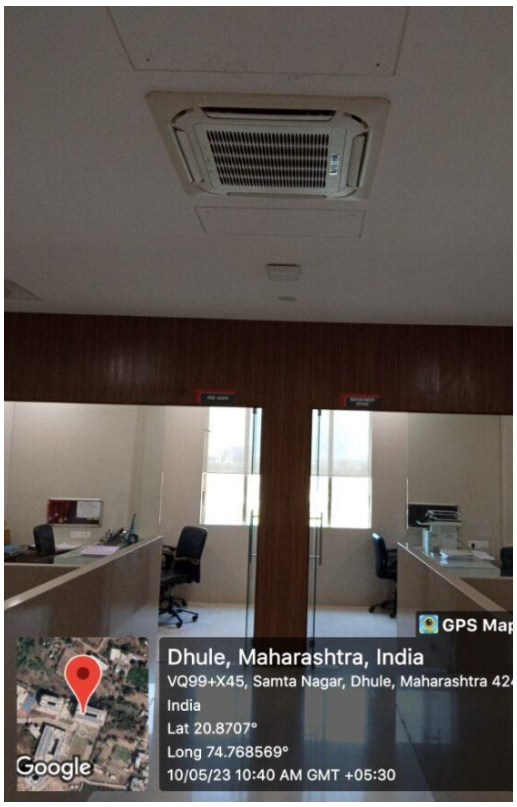
Infinite Broadnet Solution Pvt Ltd
Authorized Signatory

2. Router

Sr. No	Configuration	Quantities
01	Cisco wireless access point(Router)	80

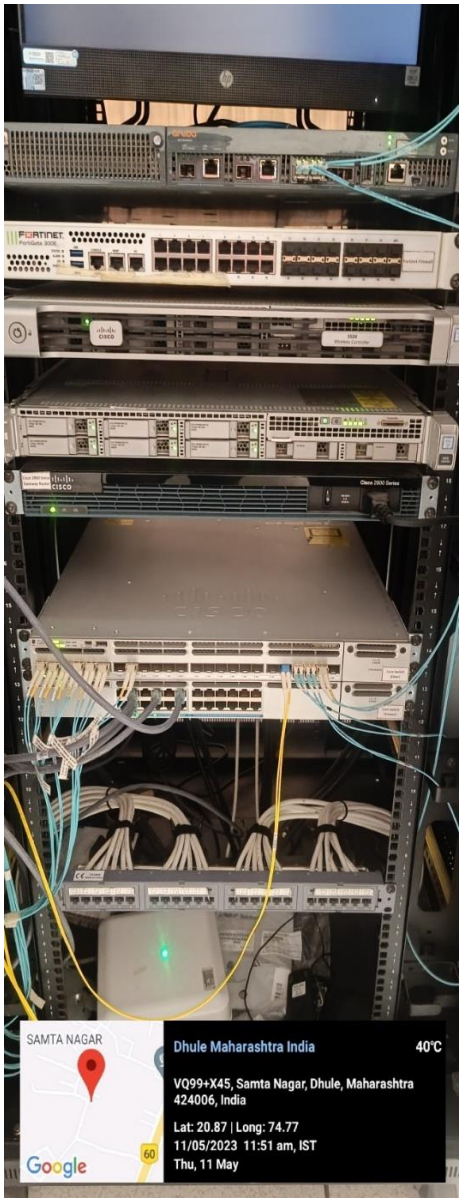


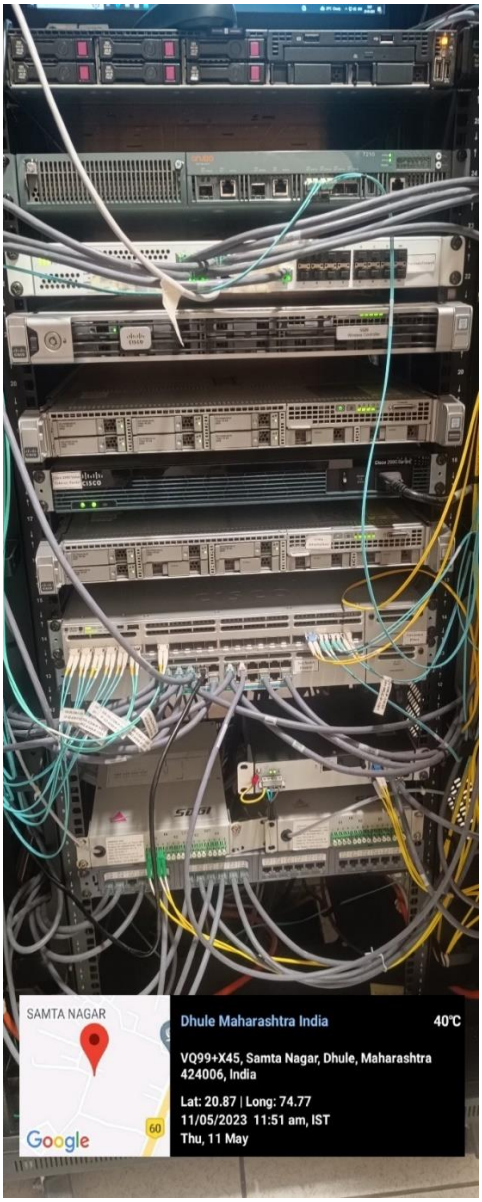




3. Switches

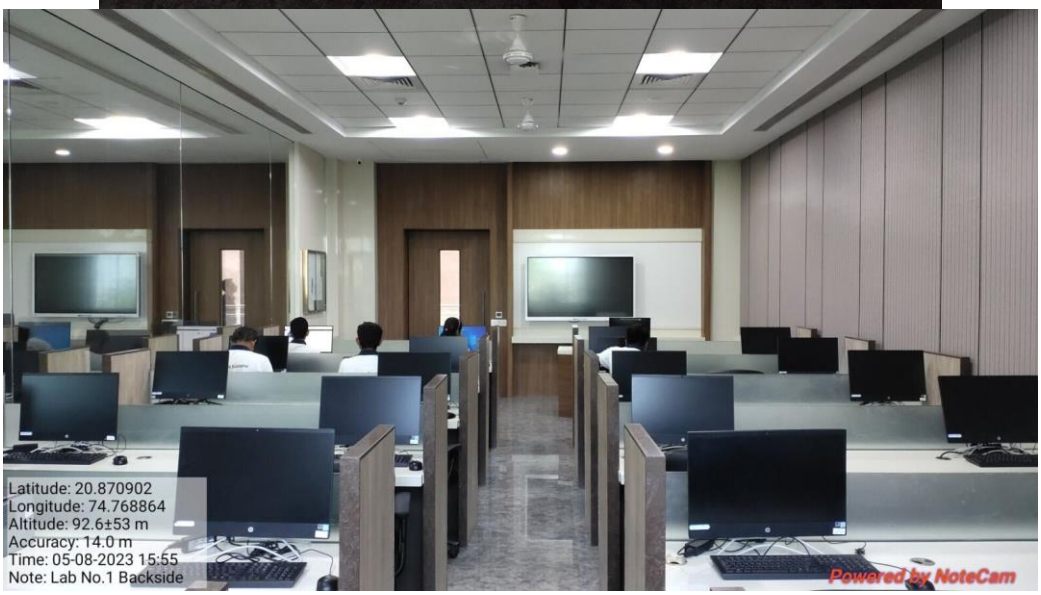
Sr. No	Switches Configuration	Quantities	Year of purchasing
1	Cisco catalyst 3850 24 mGig	2	24/10/2017
2	Cisco catalyst 3850 24 mGig	2	24/10/2017
3	Cisco catalyst 2690-X 48 GigE	10	24/10/2017
4	Cisco catalyst 2690-X 48 GigE	16	24/10/2017
5	Cisco catalyst 3560-CX 12 Port POE 10G	2	24/10/2017
6	Cisco Business Edition 6000M Svr M4	2	24/10/2017
7	Cisco 5520 wireless control	2	24/10/2017
8	Cisco Business Edition 6000M	2	24/10/2017
Total		**36**	-





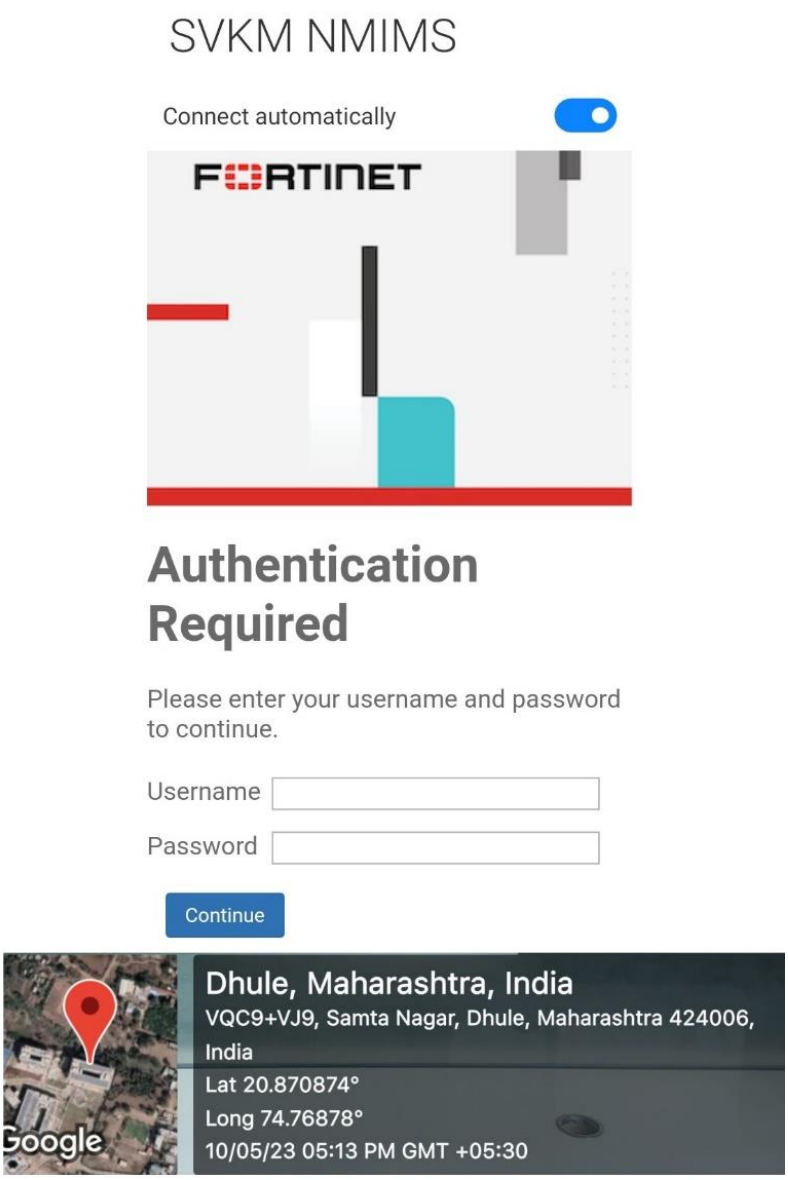
4. Computers

Sr. No	Desktop Configuration	Quantities	Year of Purchasing
1	HP 200 G3 AIO	100	14/9/2018
2	HP 200 G3 AIO	65	2/7/2019
3	HP 200 G3 AIO	50	31/10/2019
4	HP 200 G4 AIO	50	9/7/2020
5	HP 200 G4 AIO	25	15/7/2020
6	HP BU PON 600 G6 AIO	50	9/2/2022
7	Dell Optiplex 5400 AIO	208	21/02/2023
8	Dell Optiplex 5400 AIO	70	4/4/2023
Total		**618**	-



5. Firewall

Sr. No	Firewall Configuration	Quantities	Year of Purchasing
1	FORTIGATEFIREWALL(FG3H0E3917901590)	01	24/02/2021



6. Intrusion Detection System (IDS), Internet Provider Security (IPS)

Sr. No	Configuration	Quantities	Year of Purchasing
1	Intrusion Detection System (IDS), Internet Provider Security (IPS)	01	24/02/2021

License Information

Entitlement	Status	
FortiCare Support	Registered	Actions
Firmware & General Updates	Licensed (Expiration Date: 2024/03/01)	
Intrusion Prevention	Licensed (Expiration Date: 2024/03/01)	
AntiVirus	Licensed (Expiration Date: 2024/03/01)	
Web Filtering	Licensed (Expiration Date: 2024/03/01)	
Email Filtering	Licensed (Expiration Date: 2024/03/01)	
Outbreak Prevention	Licensed (Expiration Date: 2024/03/01)	

TAX INVOICE *(DUPLICATE FOR SUPPLIER)*

IRN : **5e86abbb1fafda10a2a7fa3af0d7obf21cb2d59aee5706e5a99572564bd470f2**
Ack No. : **122110585241376**
Ack Date : **2-Mar-21**

MICROPOINT COMPUTERS PRIVATE LIMITED
17 & 18, NAVKETAN ESTATE,
OPP. ONIDA HOUSE,
MAHAKALI CAVES ROAD,
ANDHERI (E), MUMBAI - 400093
TEL NO - 022 40956363/ 300
GSTIN/UIN: 27AACCM8590Q1ZK
State Name : Maharashtra, Code : 27
CIN: U72200MH2002PTC135224
E-Mail : sales@mpcl.in

Consignee (Ship to)
SHRI VILE PARLE KELAVANI MANDAL'S
SVKM's Institute of Technology
Survey No. 499, Plot No. 2,
Behind Gurudwara,Mumbai Agra National Highway,
Dhule - 424001
KA : Mr. Amol Sonawane (M) 7588629096
GSTIN/UIN : 27AABTS8228H1Z8
State Name : Maharashtra, Code : 27

Buyer (Bill to)
SHRI VILE PARLE KELAVANI MANDAL'S
SVKM's Institute of Technology
Survey No. 499, Plot No. 2,
Behind Gurudwara,Mumbai Agra National Highway,
Dhule - 424001
KA : Mr. Amol Sonawane (M) 7588629096
GSTIN/UIN : 27AABTS8228H1Z8
State Name : Maharashtra, Code : 27
Place of Supply : Maharashtra

Invoice No.	Dated
SRS-0191/20-21	**24-Feb-21**
Delivery Note	Mode/Terms of Payment
	30 Days
Reference No. & Date.	Other References
Buyer's Order No.	Dated
4600035646	**16-Feb-21**
Dispatch Doc No.	Delivery Note Date
Dispatched through	Destination
Terms of Delivery	

Sl No.	Description of Services	HSN/SAC	Quantity	Rate	per	Amount
1	**FORTIGATE RENEWAL** *Renewal Of Fortinet Firewall Till 28th Feb 2024 24x7 Comprehensive Support, Advanced Hardware Replacement (NBD), Firmware and General Upgrades, Bundle (IPS, AV, Botnet IP/Domain, Mobile Malware, FortiGate Cloud Sandbox including Virus Outbreak and Content Disarm & Reconstruct, Application Control, Web Filtering and Antispam Service)* *sr no-FG3H0E3917901590 / FG3H0E3917901072 - Standby Device* *Period-06.06.2021 to 28.02.2024*	998729	**1.0 PCS**	3,48,038.00	PCS	**3,48,038.00**
	Output CGST @ 9%			*9*	%	**31,323.42**
	Output SGST @ 9%			*9*	%	**31,323.42**
	Total		**1.0 PCS**			**₹ 4,10,684.84**

Amount Chargeable (in words) *E. & O.E*
INR Four Lakh Ten Thousand Six Hundred Eighty Four and Eighty Four Only

	Taxable Value	Central Tax Rate	Central Tax Amount	State Tax Rate	State Tax Amount	Total Tax Amount
	3,48,038.00	9%	31,323.42	9%	31,323.42	62,646.84
Total:	**3,48,038.00**		**31,323.42**		**31,323.42**	**62,646.84**

Tax Amount (in words) : **INR Sixty Two Thousand Six Hundred Forty Six and Eighty Four Only**
Company's PAN : **AACCM8590Q**

Declaration
"We hereby declare that the software items mentioned in the Invoice ar sold without any modification, the company has alredy dedcuted TDS u/s 194J of the Income Tax on these software and made necessary arrangement for remitting the same as per the time limit prescribed by Income Tax Act, 1961. PAN of the company is AACCM8590Q"

for MICROPOINT COMPUTERS PRIVATE LIMITED
Authorised Signatory

This is a Computer Generated Invoice

7. System Software

Sr.No	Description	Make	Year Of Purchasing	No Of System Software
1	MICROSOFT WINDOWS 10 PRO	MICROSOFT	14/09/2018	618
2	MICROSOFT WINDOWS 10+11 PRO	MICROSOFT	21/02/2023	618
3	UBUNTU 18.04	OPEN SOURCE	-	126
4	UBUNTU 20.04	OPEN SOURCE	-	84

8. Application Software

Sr.No	Description	Make	Year Of Purchasing	No Of Software
1	MICROSOFT WINDOWS 10 PRO (Applications)	MICROSOFT	14/09/2018	INSTALLED ON EVERY SYSTEM
2	ACROBAT DC	LDS INFOTECH PVT LTD.	23/01/2023	INSTALLED ON 136 SYSTEM
3	SYMANTIC ANTIVIRUS	JAINAM TECHNOLOGIES PVT LTD	2017 (RENEWAL 2022) 10/03/2023	INSTALLED ON EVERY SYSTEM
4	VMWARE LICENCE	LAUREN & MICROPOINT COMPUTERS PVT LTD	03/09/2020	INSTALLED ON 10 SYSTEM
5	WORDS WORTH LANGUAGE LAB SOFTWARE	ACADAMY FOR COMPUTER TRAINING(GUJ)PVT.LTD	12/12/2022	1
6	MI POWER	TECHNOSCIETIFIC COMPANY	27/08/2019	INSTALLED ON 25 SYSTEM
7	ANSYS ACADEMIC SOFTWARE	ARK INFOSOLUTION PVT LTD	31/03/2021	INSTALLED ON 25 SYSTEM
8	MATLAB	MATHWORKS	22/11/2022	ALL PC IN CAMPUS
9	TINA DESIGN SUIT	NVIS TECHNOLOGY PVT LTD	20/09/2019	1
10	STAADO PRO.	ARK INFOSOLUTION PVT LTD	07/06/2021	INSTALLED ON 25 SYSTEM

9. Smart Board

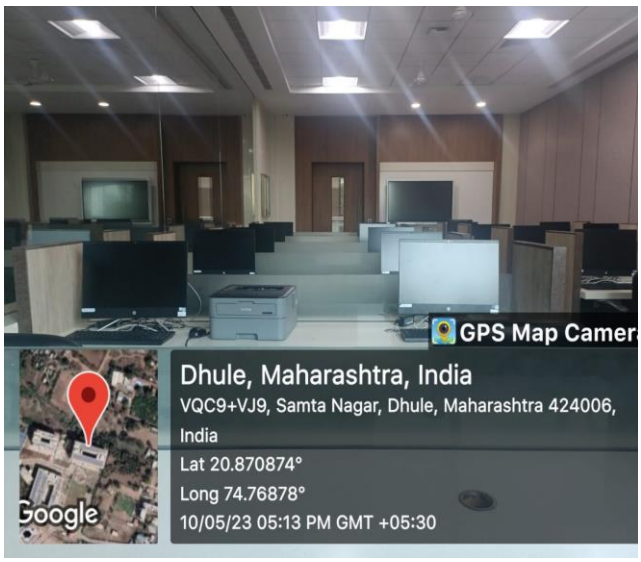
Sr. No	Configuration	Quantities	Year of Purchasing
1	Senses Intelligent Panel-65	6	17/9/2018
2	Senses Intelligent Panel-65	4	20/9/2018
3	Senses Intelligent Panel-75	7	28/08/2019
4	Smart Board(Senses Intelligent Panel-65)	11	11/3/2021
5	Senses Intelligent Panel-75	12	18/01/2022
6	Senses Intelligent Panel-75	1	25/07/2022
7	Senses Intelligent Panel-75	1	30/09/2022
8	55 Inch Smart Board	8	27/04/2022
9	Senses Intelligent Panel-75	4	24/01/2023
Total		**54**	-

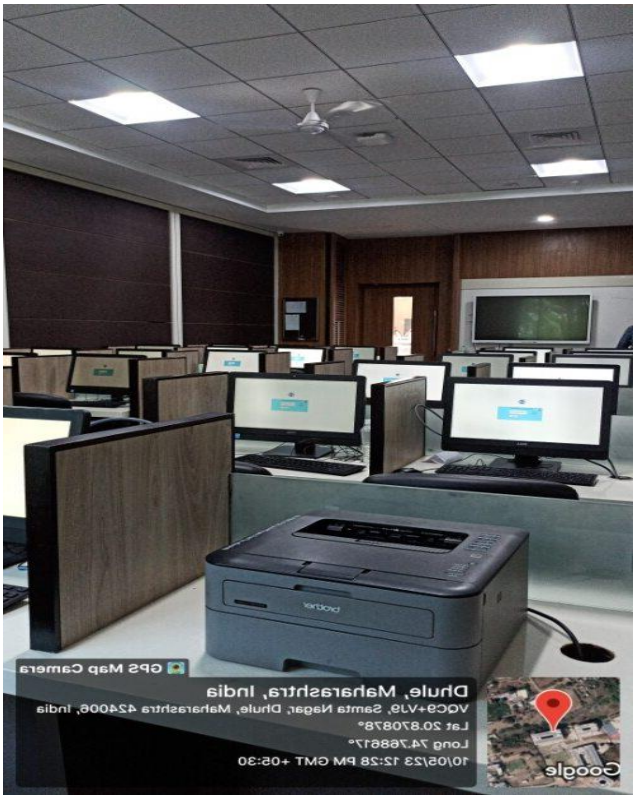
10.Projector

Sr. No	Configuration	Quantities	Year of Purchasing
1	Projector PJ X2340	09	14/02/2017

11.Printer

Sr. No	Configuration	Quantities	Year of Purchasing
1	Pinter Brother HI-L2321 LD	19	27/02/2017
2	EPSON L565	01	27/02/2017
3	Laser Jet Managed MFP E52545 HP	07	2022
Total		**27**	-





12.All in Printer (Xerox Machine)

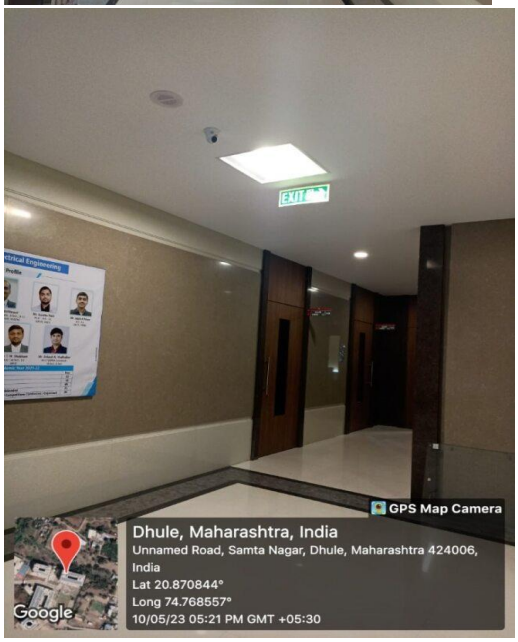
Sr. No	Configuration	Quantities	Year of Purchasing
1	PHOTOCOPIER KYOCERA TASKALFA 6501i	01	01/09/2022
2	PHOTOCOPIER KYOCERA TASKALFA 3510i	01	01/09/2022
3	Photocopier Machine(xerox machine)	01	24/04/2023
Total		**03**	-

13.Scanner

Sr. No	Configuration	Quantities	Year of Purchasing
1	SCANNER HP SCANJET 200	03	27/02/2017

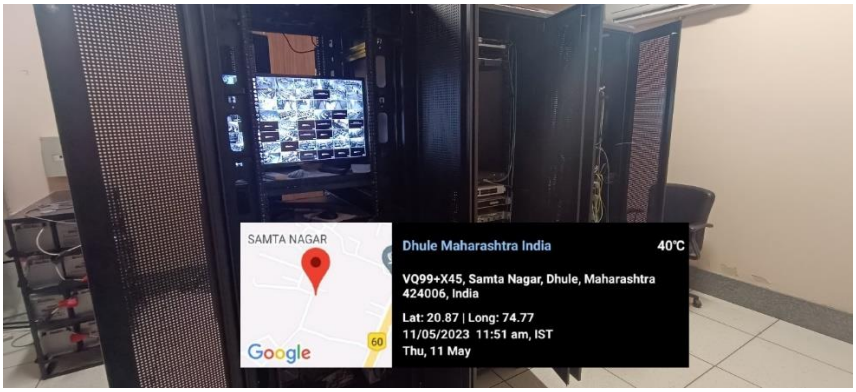
14.CCTV Cameras

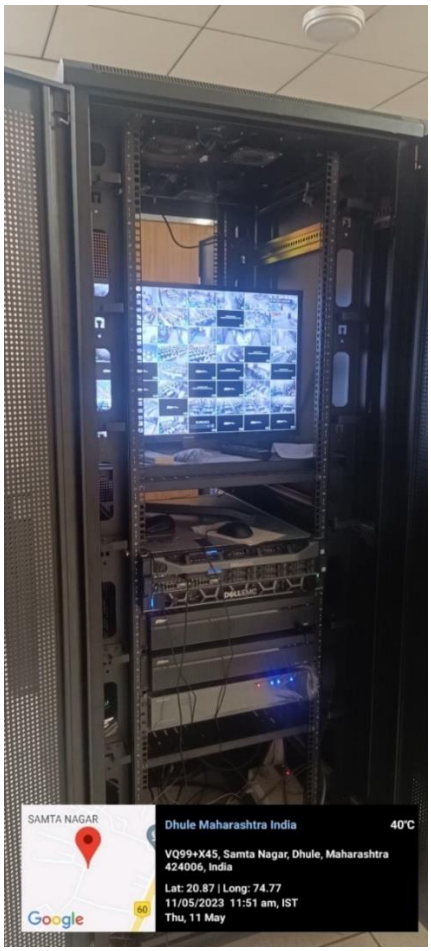
Sr. No	Configuration	Quantities	Year of Purchasing
1	CCTV Camera LNV-6010R	150	04/05/2022



15.Servers

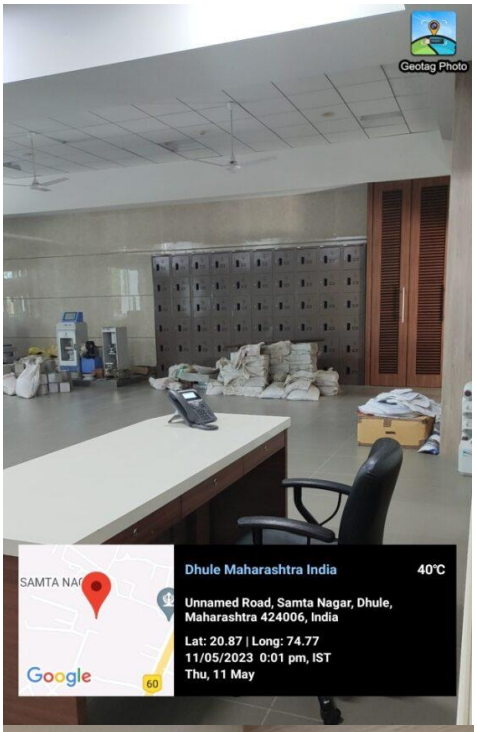
Sr. No	Configuration	Quantities	Year of Purchasing
1	DELL POWEREDGE R330 SERVER	2 PCS	30/01/2019
2	DELL POWEREDGE R440 SERVER	1 PCS	30/01/2019
Total		**03**	-

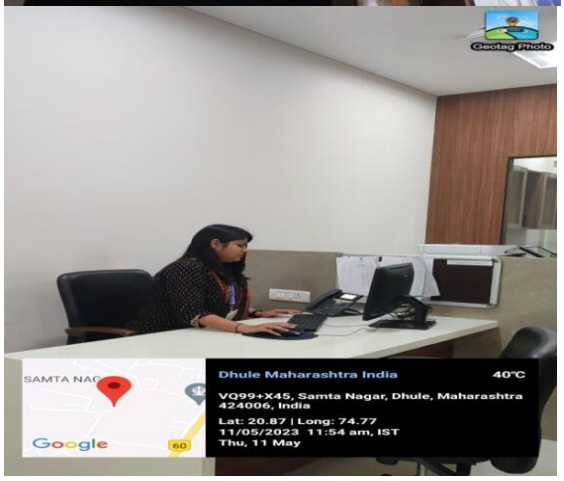




16.Telecom

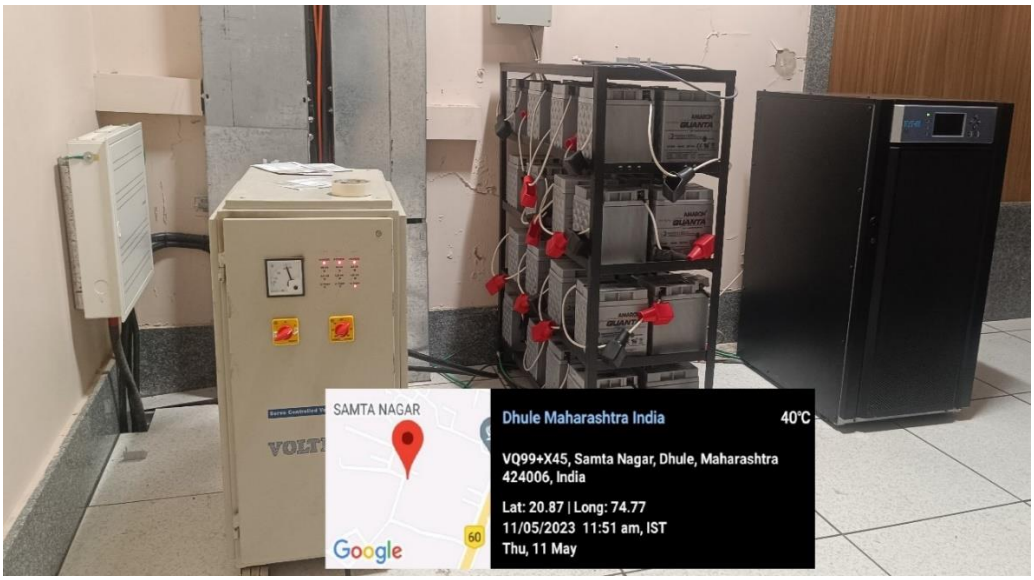
Sr. No	Configuration	Quantities	Year of Purchasing
1	Cisco UC Phone 7821	37	24/10/2017
2	Cisco IP Phone 8865	03	24/10/2017
3	Cisco IP Phone 8851	01	24/10/2017
Total		**41**	-





17.UPS

Sr. No	Configuration	Quantities	Year of Purchasing
1	93E 15 kVA UPS with MBS	02	29/05/2018



18.Laptop

Sr. No	Configuration	Quantities	Year of Purchasing
1	Lenovo VI4-IIL	01	20/09/2017