Document Name	Information Security – User Acceptance Policy
Document Number	POL-ISMS-NL-010-01
Effective date	23rd Sep 2021

Author: **ISO**	Reviewer: **IT Security Operation Forum**	Approver: **CISO**
Signature	Signature	Signature
Electronic copies valid without signature		

Document Amendment Details

Version Number	Date	Nature of Modification
1.0	29-Aug-19	Initial Draft
1.0	23-Nov-20	Annual review, no changes
1.1	23-Sep-21	Annual review, Revision to address the use of assets and updated Annexure-A

Master files are stored electronically and are available to all Associates
Printed copies of the master files are for reference only.

Table of Contents

1. Introduction

This Information Security - User Acceptance Policy for IT Systems is designed to protect, Nihilent and its employees, customers and other partners from any damage and harm caused by the misuse of IT systems and data. Misuse includes both deliberate and inadvertent actions. This policy must be read in conjunction with the Information Technology Act, 2008, other applicable laws and regulations, ethical conduct and policies to those who report to you and local laws wherever the company does business.

2. Consequences

The consequence of misuse of systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g., computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network downtime.

3. Applicability

Everyone who works for Company is responsible for the security of IT systems and the data on them. As such, all employees must ensure they always adhere to the guidelines of this policy. Any employee, if unclear on the policy or how it impacts their role, should speak to their manager or Information Security Operations Team.
This policy applies to all persons who have access to any of Nihilent Information Resources. This includes permanent employees, contractual employees, trainees, contractor, agencies, consultants, suppliers, customers, business partners and authorized guests and all persons authorized for access or use privileges by the Nihilent, hereafter referred to as “users”.
This policy applies to all locations from which Nihilent information is accessed including home use and all disciplinary action will be applied in a manner consistent with the applicable local law.

4. Resources covered

Resources covered by this policy include:
All information resources either in digital or physical format such as desktop computers, laptops, smartphones, tablets, printers, data and voice network, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, camera, internet access, applications, printed information, and all other similar items commonly understood to be covered by this term.

5. Confidentiality

All users with access to confidential data are to exercise all appropriate precautions to maintain the accuracy, integrity and confidentiality of the data and ensure that no data interference (unauthorized

damaging, deletion, deterioration, alteration of suppression of computer data), illegal access, illegal interception (non-public transmission of computer data to, from or within a computer system), system interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer system), misuse of devices, forgery (ID theft), electronic fraud and unauthorized disclosures occur.

6. Data Privacy

All users are expected to follow Nihilent's Data Privacy policies and guidelines. Please refer Data Privacy Policy (POL-DP-010) and Staff Privacy Statement (STMT-DP-050-02) for more information.

7. Nihilent rights

Company reserves the right to access, monitor and disclose the contents and activity of an individual user's account(s). This action shall be taken to maintain the network's integrity and the rights of others authorized to access the network.
Users should be aware that electronic data, software and communications files are copied to Nihilent provided secured repositories only including – Company provided OneDrive, backup systems, SharePoint and collaboration platform like Microsoft Teams. Items that were deleted shall be preserved on backup tapes and retrieved if necessary. All the activity on systems and networks shall be monitored, logged and reviewed by the system administrator, or discovered in legal proceedings. In addition, all documents created, stored, transmitted or received on Company's computers and networks shall be subject to monitoring by the systems administrator.

8. Responsibilities

Each user shall:

1. Be responsible for the security and integrity of official information stored on any type of digital devices including Desktop/ Laptop/Mobile and any other system. This includes:
   - Making regular backup of all the information and files.
   - Controlling and securing physical and network access to e-resources and data.
   - Properly logging out of sessions.
   - Monitoring access to their accounts, if a user suspects that their access codes have been compromised or that there has been unauthorized activity on their accounts, they are to report it to IT security via help desk and change their access codes immediately; and
   - Security tools recommended by the Group security office installed and updated on the assigned workstations.
2. Choose appropriate password(s), as per password policy and guard the security of that password.
3. Abide by the password protection practices specified for each E-resource and change their access codes on a regular basis, or as required by standards.

4. Use only the access codes and privileges associated with their computer account(s) and utilize those account(s) for the purposes for which they were authorized.
5. Take full responsibility, when sharing access codes and user account information, for the use of any user to whom they provided their access code.
6. Respect and honour the rights of other individuals, with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright infringement and use of E-resources.
7. Users should adhere to "User Acceptance Policy" while creating, posting, commenting, communicating, participating, or engaging in any form of conduct with respect to Nihilent's Information Resources, which include, but are not limited to mobile and computing devices, software, cloud services, network resources, social media, social networking, source code repositories, etc. Whether using the Nihilent's Information Resources or not.
8. User should use only official email accounts (provided by Nihilent-O365/client) for work-related purposes.
9. User should only use official Unified Communication and Collaboration tools like Microsoft Teams for voice, video and content sharing. Any exception to this needs to be approved by the Project Manager or higher authority based on a project or a business requirement.

9. Restrictions

Users shall not do the following:

1. Provide access codes to any user not authorized for such access.
2. Remote access authentication must not be shared with other users or non-users.
3. Make use of accounts, access codes, privileges, or E-resources to which they are no longer authorized.
4. Tampering with, modifying, or altering restrictions or protection placed on their accounts or network facilities.
5. Uses of Internet access in a malicious manner to alter or destroy any information available on the Internet or on any network accessible through the Internet for which he or she does not own or have explicit permission to alter or destroy.
6. Using knowledge of security or access controls to damage computer and network systems obtain extra E-resources or gain access to accounts for which they are not authorized.
7. Physically damaging or vandalizing E-resources.
8. Alter the source address of messages, or otherwise forging email messages.
9. Engaging in activities that harass, degrade, intimidate, demean, slander, defame, interfere with, or threaten others.
10. Commenting or acting on behalf of the Company over the Internet unless you have the authority to do so.
11. Introducing, creating, or propagating computer viruses, worms, Trojan horses or other malicious code to E-resources.
12. Gambling, inciting hate, bullying, child soliciting and abuse, identity theft, cyber terrorism, insane/obscene mail, sexual harassment at workplace or any other harassment which affect

the Nihilent's policy and work culture of workstation and sending and posing discriminatory harassing messages.

13. Place Nihilent confidential information on mobile and computing devices, database, software, cloud services, network resources, social media, social networking, source code repositories, etc.
14. Shall not disclose, copy, upload any type of Nihilent's, a customer's, or another party's sensitive information including but not limited to database, source codes, sensitive financial data, etc.
15. Place Nihilent confidential information on social media, social networking or any source version control tools, software that may exist. (e.g., Twitter, Facebook, personal websites, weblogs, GitLab, GitHub, BeanStalk, SourceForge, Bitbucket, CodePlane etc.)
16. Use social media to disparage, harass, bully, or intimidate other individuals (whether or not Nihilent Associates), or disclose Confidential Information.
17. Associates should not use their official email accounts (provided by Nihilent-O365/client):
    a. Register to illegal, unsafe, disreputable, or suspect websites and services.
    b. Send obscene, offensive, or discriminatory messages and content.
    c. Send unauthorized advertisements or solicitation emails.
    d. Sign up for a competitor's services unless authorized.
    e. Auto forward of corporate emails to personal email id unless preapproved by the Manager.
18. User should not tamper security tools or deviate any standard security settings under any circumstances.

10. Use of Company's Assets

Protection of the Company's assets is a key responsibility of every person associated with the Company. In the course of your employment with the Company you will be allowed to use the Assets and resources of the Company as per the requirements of your employment. You will be responsible for the proper use, protection and conservation of the Company's assets and resources. You must safeguard such assets against loss, damage, misuse, or theft. Care should be taken to ensure that assets are not misappropriated, loaned to others, or sold without appropriate authorization. This includes Company properties, assets, proprietary manufacturing process, engineering designs, process technology, application knowledge, financial data, strategies, trade secrets, corporate information, and other Company rights. Company assets are to be used solely to pursue and achieve Company goals and not for personal benefit.
The Company has developed procedures and control for usage and protection of company's asset.
You shall indemnify the Company if there is any loss or damage of the Company's assets, and such loss arises out of your improper usage of the Asset or non-compliance of the procedures.

10.1. Use of Customer's or Third-Party's Assets

Protection of Customer's assets is a key responsibility of the associates to whom Customer's/Third-Parties assets are allocated or under possession and control. In the course of your employment with

the Company you will be allowed to use the assets and resources of the Customer's/Third-Party's requirements. Nihilent has developed procedures and control Handling Client Furnished Items (PR-PRJ-150) for usage and protection of Customer's/Third-Party's assets.

You shall indemnify the Company if there is any loss or damage of the Customer's/Third-Party's assets, and such loss arises out of your improper usage of the Asset or non-compliance of the procedures.

11. Copyrights and licenses

Software shall not be copied, installed, or used except as permitted by the owner of the software and by law. Software, subject to licensing, must be properly licensed and all related to such license provisions (including installation, use, copying, number of simultaneous users, terms of the license, etc.) must be strictly adhered to.

All copyrighted information, such as text and images, retrieved from information-resources or stored, transmitted, or maintained with information-resources, must be used in conformance with applicable copyright and other laws. Copied material, used legally, must be properly attributed in conformance with applicable legal and professional standards.

The Information Technology (Amendment) Act, 2008, Copyright (Amendment) Act, 2012 and other applicable Acts and Laws, provide severe civil and criminal penalties for the cyber-crime and the unauthorized reproduction, distribution, or exhibition of copyrighted materials.

12. Non-organizational User

Users shall not use information-resources for:
1. Compensated outside work
2. The benefit of un-related /independent
3. Personal gain or benefit
4. Political or lobbying activities
5. Private business or commercial enterprise

Failure to abide by the rules set out above will result in penalties appropriate to the severity of the breach under various laws as enclosed in Annexure "A".

13. Disclaimer

Each user unconditionally and unequivocally agrees to take self-onerous responsibility not to disclose any of the above-referred data or any related information obtained from discussions/meetings/tele-conferencing/video-conferencing etc. and all users should use their own judgment regarding what is unacceptable use of Company's system and do not create, access, store, print, solicit or send any material that is intimidating, harassing, threatening, abusive, sexually explicit or otherwise offensive or inappropriate, nor send any false, derogatory or malicious communications.
Over time, any changes in the present User Acceptance Policy will be communicated to all concerned and all shall have to abide by these changes.

User	HR Department
_____	_____
User Signature	Signature
_____	_____
User Name	Name
_____	_____
Date	Date

14. Annexure 'A'

Sl. No.	Offences	Section under IT Act	Punishment
1	Tampering with computer source documents	Sec. 65	Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both
2	Computer Related Offences (any act referred to section 43)	Sec. 66	Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both
3	Dishonestly receiving stolen computer resource or communication device	Sec. 66B	Imprisonment for a term which may extend to three years or with fine which may extend to Rs. 1 Lakh or with both
4	Punishment for identity theft	Sec. 66C	Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to Rs. 1 Lakh
5	Punishment for cheating by personation by using computer resource	Sec. 66D	Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to Rs. 1 Lakh
6	Punishment for violation of privacy	Sec. 66E	Imprisonment which may extend to three years or with fine not exceeding Rs. 2 Lakh, or with both
7	Punishment for cyber terrorism	Sec 66F	Imprisonment which may extend to imprisonment for life
8	Punishment for publishing or transmitting obscene material in electronic form	Sec 67	Imprisonment which may extend to five years and with fine which may extend to Rs. 10 Lakh.
9	Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec. 67A	Imprisonment which may extend to seven years and with fine which may extend to Rs. 10 Lakh.
10	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Sec. 67B	Imprisonment which may extend to five years and with fine which may extend to Rs. 10 Lakh.
11	Preservation and retention of information by intermediaries	Sec. 67C	Imprisonment which may extend to three years and shall also be liable to fine

12	Powers to issue directions for interception or monitoring or decryption of any information through any computer resource	Sec 69	Imprisonment which may extend to seven years and shall also be liable to fine
13	Power to issue directions for blocking for public access of any information through any computer resource	Sec 69A	Imprisonment which may extend to seven years and shall also be liable to fine
14	Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security	Sec. 69B	Imprisonment which may extend to three years and shall also be liable to fine
15	Un-authorized access to protected system and establishment	Sec. 70	Imprisonment which may extend to ten years and shall also be liable to fine.
16	Penalty for misrepresentation	Sec. 71	Imprisonment which may extend to two years or with fine which may extend to Rs. 1 Lakh or with both
17	Punishment for disclosure of information in breach of lawful contract	Sec. 72A	Imprisonment which may extend to three years or with fine which may extend to Rs. 5 Lakh or with both
18	Publishing False digital signature certificates	Sec. 73	Imprisonment which may extend to two years or with fine which may extend to Rs. 1 Lakh or with both
19	Publication for fraudulent purpose	Sec. 74	Imprisonment which may extend up to two years or with fine which may extend up to Rs. 1 Lakh or with both
20	Act to apply for offence or contraventions committed outside India	Sec. 75	Punishment depends on offence committed under the jurisdiction, territory and nationality
21	Exemption from liability of intermediary in certain cases	Sec. 79	
22	Punishment for abetment of offences	Sec. 84B	Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment and no express provision is made by this Act for the punishment of such

			abetment, be punished with the punishment provided for the offence under this Act.
23	Punishment for attempt to commit offences	Sec. 84C	Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.
24	Offences by Companies	Sec. 85	Every person who, at the time the contravention was committed, was in charge of and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly

Note: Sec.78 of IT Act empowers Police Inspector to investigate cases falling under this Act.

25	Sale, etc., of obscene objects to young person	Sec. 293 IPC	Imprisonment of either description for a term which may extend to three years and with fine which may extend to two thousand rupees.
26	Obscene acts and songs	Sec. 294 IPC	Imprisonment of either description for a term which may extend to three months, or with fine, or with both.
27	Web-Jacking (Extortion)	Sec 383 IPC	U/s. 384 of IPC, whoever commits extortion shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
28	Bogus websites, Cyber Frauds	Sec. 420 IPC	Imprisonment for a term which may extend to seven years and shall also be liable to fine.
29	Sending defamatory messages by e-mail	Sec. 499 IPC	U/s. 500 of IPC, whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

30	Sending threatening messages by e-mail	Sec. 503 IPC	U/s. 506 of IPC, whoever commit the offences shall be punished with imprisonment for a term which may extend to two years, or with fine, or with both
31	Criminal intimidation by an anonymous communication	Sec. 507 IPC	Imprisonment for a term which may extend up to two years
32	E-mail Spoofing	Sec. 463 IPC	U/s 465 of IPC, whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
33	Making a false document	Sec 464 IPC	U/s 465 of IPC, whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
34	Forgery for purpose of cheating	Sec. 468 IPC	Whoever commits forgery, intending that the document forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years and shall also be liable to fine.
35	Forgery for purpose of harming reputation	Sec. 469 IPC	Whoever commits forgery, intending that the document forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine.
36	Word, gesture or act intended to insult the modesty of a woman	Sec. 509 IPC	Simple imprisonment for a term which may extend to one year, or with fine, or with both.
37	When copyright infringed: - Copyright in a work shall be deemed to be infringed	Sec. 51, Copyright Act	U/s 63 of Copyright, whoever commit copyright infringed, punishable with imprisonment for a term of which not less than six months but which may extend to three years with fine not less than Rs. 50,000/-
38	Offence of infringement of copyright or other rights conferred by this Act. Any person who	Sec 63, Copyright Act	

	knowingly infringes or abets the infringement of		
39	Enhanced penalty on second and subsequent convictions	Sec 63A, Copyright Act	
40	Knowing use of infringing copy of computer program to be an offence	Sec. 63B, Copyright Act	
41	Theft of Computer Hardware	Sec. 378, IPC	Whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
42	Punishment for theft	Sec. 379, IPC	
43	Online Sale of Drugs	NDPS Act	Punishment range imprisonment from 15 to 30 years for any subsequent offences together with monetary fines
44	Online Sale of Arms	Arms Act	

15. Annexure 'B'

Key Definitions

- **Cloud Services** are applications, or other ICT (information and communication technology) resources hosted on or accessed via the internet.
- **Information Systems** are Information Communication Technology system or components of systems including, but not limited to computers, software and network resources such as internet, email and voicemail, and mobile devices including phones, smartphones and tablets.
- **Social Media and Social Networking** are interactive computer-mediated technologies that facilitate the creation and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks (e.g., Twitter, Facebook, WhatsApp, Instagram, Google+, Skype, LinkedIn, Telegram, Reddit, YouTube, TikTok, etc.)
- **Source Code Repositories** tracks collaborative changes made and ensures each collaborator is aware and has access to the project's most recent version. (e.g., AWS Code Commit, GitLab, GitHub, Beanstalk, Source Forge, Bitbucket, Code Plane, etc.)
- **Access code** is an identification number and/or password used to gain access into a computer system.