Acceptable Use Policy

INTERNAL USE

All Rights Reserved: Netsmartz House, Plot No. 10, Rajiv Gandhi I.T. Park, Chandigarh

Document Vérification & Version Control		
Issuing Authority:	***Information Technology Division***	
Version No.:	***1.1***	
Release Date:	***13-Sept- 2018***	
Authored by	***Name:***	***Samrat Sheel Sharma***
	Signature:	***S.S.Sharma***
	Date:	***13-Sept-2018***
Approved by	***Name:***	***Vikas Katoch***
	Signature:	
	Date:	

Uncontrolled copy if printed/ photocopied (unless specified otherwise)

NOTICE:
Information contained in this document is classified Netsmartz Confidential Proprietary. No person outside the Netsmartz, LLC shall have access to the information contained in this document unless business needs dictate, otherwise. It is the responsibility of the person knowing the information contained in this document to ensure confidentiality of information contained in it and preventing unauthorized access to this document at all times.

INTERNAL USE

Amendment Record			
Document Version/Revision	**Author(s)**	**Date**	**Amendment Details**
0.0	Samrat Sheel Sharma	13-Sept-2018	Published
0.1	Samrat Sheel Sharma	15-07-2022	New Helpdesk System

Table of Contents

INTERNAL USE

Contents

Overview

Netsmartz intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to NETSMARTZ's established culture of openness, trust, and integrity. Netsmartz is committed to protecting NETSMARTZ's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of NETSMARTZ. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every NETSMARTZ employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at NETSMARTZ. These rules are in place to protect the employee and NETSMARTZ. Inappropriate use exposes NETSMARTZ to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct NETSMARTZ business or interact with internal networks and business systems, whether owned or leased by NETSMARTZ, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at NETSMARTZ and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with NETSMARTZ policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at NETSMARTZ, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by NETSMARTZ.

INTERNAL USE

Introduction

This document is divided into guidelines mentioned below and should be actively read along with Netsmartz Acceptable Use Policy.

- Email Guidelines
- System Guidelines
- Network and Internet Guidelines
- Security Guidelines
- Telephone Guidelines

An e-mail is sent to all new employees when they join.

Dear New Employee,

Congratulations on your employment at Netsmartz Infotech India Pvt. Ltd. We look forward to helping you in setting up the required resources and maintenance.

IT Team is responsible for securing the network and maintenance of systems and servers. This document guides you into the details of Information Technology (IT) related resources.

Wish you all the best and good luck for your career in Netsmartz!

Email Guidelines

Netsmartz email guidelines are designed to take care of the needs of our employees as well as our customers. The norms, to which each of you should comply, are mentioned below:

NTZ_ITD_AUP_1.1_005

INTERNAL USE

You can send emails of up to 6 MB only, including the message body and attachments.

You can receive emails of up to 6 MB only, including the message body content and attachments.

By default, Thunderbird will be configured as email Client with Open Office. The protocols supported to download mails are POP, RPC over HTTP and HTTPS.

You can access the mail service from outside the Netsmartz network by using the URL https://outlook.office365.com for .com IDs and http://mailzimb.netsmartz.net for .Net Email Ids. The mailing system is monitored, and the log will be screened for all employees, to make sure that the resource is used efficiently.

Any notification to be sent to all employees of Netsmartz must be directed through HR, IT and Admin department.

You can reach IT Support by logging your request through email at https://netsmartz.darwinbox.in/user/login

To Process Registered Service request kindly mention necessary details like Cubical location ,contact number along with brief problem description.

Do not add disclaimers to your signature, as it is taken care at the server end.

System Guidelines

IT admin will share your login ID and the default password while assigning the system & make sure to change your password. Memorize your credentials and do not share it with others.
Mandatory to use project approved software application on the official systems and do not install crack or trail versions at your own.

By default, you have all the permissions to install new applications, Security Patches, and Critical Updates on your local system. The updates are pushed from the central server. Users are advised to install the updates without fail and update IT Support in case of any errors noticed during the installation. The password should be of at least 8 to 10 characters which should be a combination of capital and small letter, minimum one numeric and special character is necessary. The password will expire after 60 days, and user receives an automated mail from the admin 15 days prior to the expiry date.

INTERNAL USE

•Always check the Antivirus Software, which is updated automatically, failing which, you must bring it to the notice of IT Support at INFOSEC@netsmartz.com

•Any requirement for software or hardware must be requested through Helpdesk portal https://netsmartz.darwinbox.in/user/login
duly Approved from reporting Manager.

•Installation of any third-party application requires approval from your Project Manager. Any application, which is not concerned to the project, will be removed from the system without any prior notice to the user.

•You should not move the system to any other cubical other than the one allotted to you. In case you are required to move, then raise a request to the admin group at and specifying the reason for movement.

•Any upgrades or request for additional system must be brought to the notice of IT Support, a minimum of 4 days in advance with prior approval from your Reporting Manager.

Network and Internet Guidelines

- You strictly must not change the IP address settings of your system.
- Project related data are stored at centralized location on servers. You must access the same using client applications like TFS, Database or Share Point Access. Permission to access these data on the server will be given only on approval from your Reporting Manager.

- Access to any of the network printers will be denied, by default and will be given by IT Team. Printing of personal documents like resumes, books, etc. are strictly prohibited, and usage of each user will be monitored.

- If a client wants to access your workstation remotely to view a project demo or for any other reason, then you must send a request specifying the complete details by filling the checklist (Checklist for Firewall External Mapping). IT will suggest a suitable mode of sharing the system and handle the request. You will be provided with necessary details to access the system remotely, which in turn can be shared with the client.

INTERNAL USE

- Access to browse technical and informative sites on the Internet has been allowed for all. Entertainment and media URLs will not be entertained. Any URL of technical sites, which proves necessary for project purpose and is not accessible, can be sent to IT by getting approval from their reporting manager. The same will be allowed on Firewall. By default, the uses of messengers have been denied. Users, who want to communicate with clients can avail this facility on approval from their Reporting Manager. The sites are blocked based on the reputation and the category they belong to. Any above said such services are allowed for three months only and must be renewed after that.

- For any download of software or other data from the Internet, request must be made at helpdesk portal https://netsmartz.darwinbox.in/user/login Request will be processed by IT and the link to obtain the downloaded data will be sent to the user.

Security Guidelines

- All users are bound to group policies, wherein, access to all the shared folders on Netsmartz Intranet depends on the level of access permissions they have. Any request to access the shared folders must be directed to IT with approval from the Reporting Manager. Auditing is enabled on all the shared folders to avoid mishandling of crucial data.

- To transfer bulk data over the Internet, we have a FTP server, each project can have its account created on the FTP server whenever there is a need to share data outside the network. Credentials to access the FTP server will be given only to concerned users of the project. It is the responsibility of every user to maintain the information with utmost secrecy. By default, the password will expire every 60 days - you must set reminders and update IT to reset it well in advance to avoid any circumstances.

- IT Team provides **VPN service** for users, who work from home or on-site, based on their Reporting Manager's approval.

Telephone Guidelines

The PSTN lines have been facilitated in cubicles and can make calls.
Usage of each workstation will be monitored through System and all employees are bound to follow Netsmartz Security Policy.

INTERNAL USE

Computer Hardware Usage Policy

Mandatory to all PC's (including the monitors) should be powered off when not in use. The benefits of doing this include:

- Security - if a machine is switched off it cannot be infected with viruses or be hacked.
- Power saving - a switched off machine will use very little power - saving energy, money, and the environment. By taking the additional step of switching off the power at the socket, you can reduce power usage to zero.
- Updates – Microsoft provide regular updates and the majority are applied when you start your machine up. Regularly shutting down your machine means you will be ensuring that it is fully up to date.

INTERNAL

- NETSMARTZ proprietary information stored on electronic and computing devices whether owned or leased by NETSMARTZ, the employee or a third party, remains the sole property of NETSMARTZ. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*
- You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of NETSMARTZ proprietary information.
- You may access, use, or share NETSMARTZ proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within NETSMARTZ may monitor equipment, systems, and network traffic at any time.
- NETSMARTZ reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of NETSMARTZ authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NETSMARTZ-owned resources.
The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

INTERNAL USE

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NETSMARTZ.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NETSMARTZ or the end user does not have an active license is strictly prohibited.
- Accessing data, a server, or an account for any purpose other than conducting NETSMARTZ business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a NETSMARTZ computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local Jurisdiction.
- Making fraudulent offers of products, items, or services originating from any NETSMARTZ account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.

INTERNAL USE

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the NETSMARTZ network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, NETSMARTZ employees to parties outside NETSMARTZ.
- When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within NETSMARTZ's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NETSMARTZ or connected via NETSMARTZ's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

INTERNAL USE

Important URL's recommended to add in Favorites

\\192.168.10.26\How_To_Do : Information Resources Guidelines

INTERNAL USE