सत्यमेव जयते

भारत सरकार / *GOVERNMENT OF INDIA*
विकास आयुक्त का कार्यालय/ *OFFICE OF THE DEVELOPMENT COMMISSIONER*
सीप्ज़ विशेष आर्थिक क्षेत्र/ *SEEPZ SPECIAL ECONOMIC ZONE*
वाणिज्य एवं उद्योग मंत्रालय / *MINISTRY OF COMMERCE & INDUSTRY*
अंधेरी (पूर्व), मुंबई - 400 096 / *ANDHERI (EAST), MUMBAI – 400 096.*
टेली / *Tel* : 022-28294757
ई-मेल /*E-mail* : *dcseepz-mah@nic.in* वेबसाइट / *Web-site* : *www.seepz.gov.in*

F.No: SEEPZ-SEZ/ Admin-14011/3/2021-ADMIN/21981 Date: 01/12/2022

OFFICE ODER No.400/2022

Sub: Notification of Standard Operating Procedure For Exit Employees and NIC Email Policy for SEEPZ SEZ.

Attention is invited to the Notification 2(22)/2013-EG-II dated October 2014 and the directions of the Competent Authority, that, all staff of SEEPZ SEZ Mumbai should adhere to the standard operating procedure for exit from SEEPZ and NIC Email policy for handling "gov.in" domain email id's. Details enclosed as given below :-

1) Refer Annexure A for Standard Operating Procedure for Exit Employees.

2) Refer Annexure B for NIC Email Policy for SEEPZ SEZ.

For further clarification please contact below mentioned department.

Division – IT SEEPZ MUMBAI
Tel – 022-28294721(09 AM to 06 PM) (Monday to Friday)
Email id - gs.bhandari12@nic.in, Raman.Ghosh@gov.in, Mayur.Gadage@gov.in, Amit.Shirvalkar@gov.in, Vikram.Satre@gov.in, Vishal.chormare@gov.in .

This issues with the approval of the Competent Authority.

26/12/2022

(Dr.Vijaykumar Londhe)
Asstt. Development Commissioner
SEEPZ-SEZ, Mumbai

डॉ. विजयकुमार रोहिदास लोंढे, पीएच.डी.(लॉ)
Dr. Vijaykumar Rohidas Londhe, Ph.D.(Law)
सहायक विकास आयुक्त
Assistant Development Commissioner
सीप्ज़-सेज़, मुंबई - 96
SEEPZ-SEZ, Mumbai - 96

To:

1. All Officers & Staff Member of SEEPZ-SEZ

Annexure A) : Standard Operant Procedure for Exit Employees in SEEPZ SEZ, Mumbai

1) Purpose :

To deactivate all the login accounts of exit employees on cessation of the contractual or term deputation of the employee in SEEPZ,SEZ administration.

2) Scope :

In the event of any Outsourced staff's service on contract being discontinued it shall be incumbent on the IT Division official by way of office order assigned responsibility thereof to deactivate employee government email account , disable passwords deactivate E-Office accounts, deactivate Domain Accounts.

3) Procedures

- 3.1 Resignation / Discontinued /Exit of outsourced staff.

The IT professionals have the important job of keeping the company secure. When an employee Outsourced staff resigns / Discontinued / Exits from office, HR executive shall communicate with the IT department so they can plan for the appropriate time to disable passwords, remove government email accounts and Domain Account, collect assets (laptops, cell phones, thumb drives), and provision equipments for the replacement employee.

Tasks for the HR Executive	Tasks for the IT Executive
➢ Communicate through mail with IT Cell with a copy of the termination order of the said employee	➢ Disable passwords, Deactivate government Email id, Deactivate E-office account, Deactivate Domain Account.

Annexure B) : NIC E-mail Policy Of SEEPZ SEZ, Mumbai

1. Guard yourself against Phishing

a) Common email scams employ email messages and even websites that look official, but are in fact attempts to steal your identity to commit fraud. This is the activity commonly known as phishing.

b) Contact us immediately If anyone or a website demands personal email information/credentials by calling us or sending a screenshot of the page to support@gov.in (1800-111-555)

c) Never click on a link within an email requesting that you enter your username, password, etc. The link can also be malicious.

d) If you have any doubts about whether an email is real, contact us directly to double check. Do not open any 'fishy' emails.

e) Install a web reputation filter on your desktop that alerts users to phishing websites.

f) Make sure that you have unique username and passwords for each account/website you regularly visit.

g) Never give out sensitive personal or account information to someone that asks via email unless you have verified the message's authenticity.

2. Change your password on regular basis as per the password policy.

It is recommended to change passwords on a regular basis. In order to know the steps How to change the password Go to the home page http://mail.nic.in or http://mail.gov.in .Click on the Link Nice mail FAQ and click on how to change email password

3. Do not share your password with anyone.

Don't share your password. Do not be duped by malicious e-mails asking you for your password. This is a well-known, trick designed to fool you into sharing your password. As a rule, never share it with anyone.

4. Always remember to sign out properly after using your mail account.

Always log out of your email when finished, whether you are using web mail or POP mail. It is also recommended to log out whenever you have to leave your computer unattended for a considerable period of time.

5. Do not save or remember your password anywhere.

Do not save / remember your password anywhere (say your browser).

6. Use Anti-Virus software & update it on regular basis.

It is also highly recommended to install and maintain a anti-virus software on your computer to prevent infection from USB drives, CDs or DVDs and so on. Make sure it is updated regularly. Scan all attachments with a virus program before downloading/executing any, even if they come from someone you know.

Computers that are infected with spyware/key loggers record every word that users are typing, hence a daily scan is recommended.

7. Update the operating system and application patches

Users need to ensure that their desktop/laptop has the latest operating system and application patches. If the patch levels are not updated, updated anti-virus software will not be able to prevent an infection. Both anti-virus and operating system patches need to work together.

8. Never open / respond any mail / attachment from unknown sender.

If it happens that a few spam mails do manage to sneak through, make it a must to delete all them. Replying / Opening such emails / attachments typically only informs the sender that they have found an active email address to send more spam emails or They may contain what are known as "letter bombs" or "viruses," which can damage your PC.

9. Never subscribe your email ID on unsafe locations (over internet).

Never subscribe your email address on any unsafe / fake website, they may try to flood your inbox or spammers will try to send bulk spam mails (which may contain virus).

10. User's Role

a) The User is responsible for any data/e-mail that is transmitted using the Gov e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b) Sharing of passwords is prohibited.

c) The user's responsibility shall extend to the following:

i. Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.

ii. The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.

iii. Back up of important files shall be taken by the user at regular intervals. The IA shall not restore the data lost due to user's actions.

11. Responsibilities of Users

a) Appropriate Use of E-mail Service

i. E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ID's should be used for official communication and name based ID's can be used for both official and personal communication.

b) Examples of inappropriate use of the e-mail service

i. Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.
ii. Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.
iii. Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity.
iv. Creation and exchange of information in violation of any laws, including copyright laws.
v. Willful transmission of an e-mail containing a computer virus.
vi. Misrepresentation of the identity of the sender of an e- mail.
vii. Use or attempt to use the accounts of others without their permission.
viii. Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc.
ix. Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

12.Kavach Authentication

a) General

When you use Kavach Authentication (App), some personal information is collected from and about you. We are committed to protecting the security of this information and safeguarding your privacy. This privacy policy sets out the details of the personal information collected, the manner in which it is collected, by whom as well as the purposes for which it is used.

b) What is kavach ?

Kavach provides two-factor authentication to the user for accessing their government email service.

c) What accesses do we need?

Kavach is a mobile app that uses certain features of your device for ensuring your user registration/enrolment. . We access your device's basic information in order to complete your registration and bind your device to your user id.

d) Do we share your application data with anyone?

No. Kavach is a security app and ensures that none of your data is shared with anyone.

Signed by Dr. Vijaykumar
R. Londhe
Date: 26-12-2022 12:06:08
Reason: Approved