NATIONAL COMMISSION FOR HUMAN RIGHTS

NATIONAL COMMISSION FOR HUMAN RIGHTS PAKISTAN

IT POLICY

Compiled by: Asif Iqbal

NCHR IT Policy

This document establishes the policy of the National Commission for Human Rights regarding the management of IT resources owned and administered by its IT Department. The IT Department provides these resources to enable the effective and efficient work of NCHR staff

The primary aim of this policy is to ensure the proper utilization of NCHR's IT systems and services and to inform users about what the Commission considers acceptable use of its IT infrastructure.

This IT acceptable use policy is designed with consideration for the diverse ethnicities, cultural values, and Islamic principles of our nation, in alignment with the Pakistan constitution. The IT Department of NCHR reserves the right to modify this policy, in collaboration with the executive, as deemed necessary. Users will be duly notified of any amendments.

Any evidence of illegal activities or policy violations will be promptly reported to the appropriate authorities. Depending on the severity of the violation, actions such as access revocation and/or account suspension will be taken by the IT Department in coordination with relevant departments, the security department, and the Executive Director.

Table of Contents

Introduction

The National Commission for Human Rights (NCHR) information systems and the data contained in those systems are valuable resources and must be protected from unauthorized or improper access, use, modification, or destruction. The following policies and guidelines define the acceptable and proper use of these resources. Using these resources appropriately can enhance business and add value to the work that is done at NCHR. Inappropriate use can result in damage to systems, unwanted liability, loss of money, unauthorized disclosure of confidential information, and, possibly, civil and/or criminal liabilities. National Commission for Human Rights will revise this policy from time to time as business requirements change.

These policies and guidelines apply to information processed, created, collected, stored, retrieved, transmitted, printed, read, or displayed on any computer or electronic communication system or device. This includes, but is not limited to, workstation, portable computers and hand-held devices, voice mail, electronic mail (e-mail), fax, video, and network systems that are owned, operated, leased, or used by NCHR or any of its affiliates. These policies and guidelines apply to all "authorized individuals," that includes, but is not limited to, all those classified as employees, independent contractors or consultants.

General Guidelines

All information created, stored, read, and/or manipulated on any computer owned, leased, or used by the National Commission for Human Rights, whether on-site or off-site, by employees or any other authorized individuals as a part of their employment or under contract, is the property of the Commission. This includes any copyright or other intellectual property interest associated with such information. Copying, disclosing, transmitting, or otherwise using such information outside the scope of the user's duties and responsibilities at NCHR without permission is prohibited.

All electronic communication accounts established for NATIONAL COMMISSION FOR HUMAN RIGHTS and its employees, including but not limited to e-mail, Internet, social media, website and other online service accounts; voice mail; telephone numbers; and NCHR billed phone are the property of the Commission. NCHR reserves the right to limit or deny access of any individual to any of its computers, networks, other electronic

components, data, software, and electronic communication accounts. NCHR reserves the right to inspect, to the extent allowed by law the contents of any information created, stored, or manipulated on Commission computers or in any form of electronic communication sent or received through its computers or computer based systems.

Inappropriate Usage

The following specific types of IT System usage are not authorized and represent inappropriate use. These uses are prohibited.

- Use That Impedes or Causes Harm to the Activities of Others

Any action that denies or interferes with (or attempts to deny or interfere with) service to other users in any way is prohibited. This includes, but is not limited to:

- Excessive use of network resources through the use of on-line radio stations or use of websites that use a constant stream of network bandwidth for things like full motion video broadcasts.
- Misuse of mailing lists, propagating “chain letters” or virus hoaxes, “spamming” (spreading e-mail or postings widely and without good purpose) or “bombing” (flooding an individual, group or system with numerous or large e-mail messages).
- Knowingly distributing unwanted mail or other unwanted messages.
- Use of NCHR systems to conduct personal business.

Use that is Inconsistent with Non- Profit Status

- Commercial use of IT systems for non-Company purposes, except if specifically authorized and permitted under IT-of-interest, outside employment and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers NCHR’s educational, administrative, research and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.
- Use of IT systems in a way that suggests endorsement of any political candidate or ballot initiative. Users must refrain from using IT systems for the purpose of lobbying

that connotes involvement, except for authorized lobbying through or in consultation with INTERMEDIA's senior management.

Harassing or Threatening Use

Any harassing or threatening use of IT systems is prohibited. This includes, but is not limited to:

- Display of offensive, sexual material in the workplace.
- Procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Use Damaging the Integrity of NCHR's OR Other Systems

National Commission for Human Rights recognizes the importance of preserving the privacy of users and data stored in IT systems. NCHR employees should also be respectful of the IT systems at any other location where they utilize IT equipment.

Use in Violation of Law

Users must not use IT systems in any way that violates civil or criminal law at the federal, provincial or local levels. Examples of such uses are: promoting or distributing Illegal obscenity; receiving, transmitting or possessing child pornography; infringing Copyrights; making bomb threats etc.

Computer Usage Policy

Standard Laptop and Desktop Computer Specification:

Depending on the nature of work, computer specifications will be provided keeping in mind the availability of the technology in the local market. Minimum specifications of a standard laptop and desktop are , multicore processor, up to 8GB DDRIII RAM, 512GB SSD, 17"-19"LCD Monitor (in case of Laptop the LCD monitor starts from 12.1" to 14.3") bigger display will be provided upon request and approval . All the computer will be

loaded with latest and licensed software a standard computer will be installed with at least, windows 10 (Professional & Ultimate and enterprise edition is recommended), MS office 2019 or latest, Antivirus with real-time virus, spyware protection and internet security capable, Skype. Depending of the nature of job other software like adobe audition, adobe Photoshop, adobe premiere antivirus, will be installed.

Laptop Computer Allocation:

Only those positions between the Chairperson and managers are eligible for an official laptop computer, however this doesn't mean that laptops computer will be allocated to every staff member in these bands. Laptop will be allocated to staff members based on the nature of work and tasks of their positions well as available equipment.
Department heads will be responsible to send their requests for the allocation of the laptops to the eligible staff members within their department to Chairperson and for review and recommendations.
For the allocation of laptop to staff members below the manager grade department head will send the request with strong justification to Chairperson for reviews and recommendations.

Staff Member's Responsibility for Laptop Computers:

When official laptop computer is assigned to a staff member, they must take responsibility for it. By signing an asset issuance form the staff member acknowledged that he/she is responsible for paying for repair or replacement for laptop computer that has been lost or damaged

Desktop Computer Allocation:

Desktop computer will be issued to staff below the rank of manager depending on the nature of job, department manager will raise a request for the desktop for the staff and after approval the system will be issued.

Staff Member Responsibility in Term of Use:

It is responsibility of the user to refrain from accessing information from attaching the media (USB, CD, and External Hard Drives) to official computer which might contain potential viral threats attached. Update the virus definition on regular bases in order to be

safe from these virus threats. Loss or damage of any computer/laptop will be subject to inquiry by the IT Department and if need be the person responsible for the loss will be tasked with replacement of the item damaged/lost.

General User Guidelines:

Staff members must insure that the operating system, virus definition, operating system and other software installed are up to date, contact IT person if there is any problem with “automatic updating “feature.

Traveling With a Laptop Computer:

Laptops are prime targets for thieves lurking in airports, conference centers and hotels. Few things of such high-value are so vulnerable, and thieves know it. Laptops are carried through public areas and often used at odd places at all hours. Their users are apt to be distracted by flight schedules, appointment calendars or security personnel. This makes laptops easy targets. Never leave your laptop unattended. Laptop theft is hard to trace. What you may lose in terms of data may be even more important than the cost of the computer itself.

Staff members must ensure to back up their computer on regular bases, staff members are requested to not keep personal information on the NCHR laptop/desktop computers as this takes up hard drive space that is needed for official business, and also there is chance of affecting your personal privacy.

All supervisors of leaving staff will make sure that all the relevant data backup is handed over to them, IT department will facilitate this process.

Internet Usage Policy

Internet access is given to NCHR employees to aid in the ease of conducting business. Personal Internet access is a privilege and must be used in moderation and regarded with the strictest of care. All Internet data that is written, sent, received or displayed through NCHR computer systems are official records.

Employees must not visit sites that contain content that could be considered discriminatory,

Offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or any other person, or that could put the computers on the network vulnerable to become infected with viruses or spy-ware.

Employees should never publish to the internet any content that is not his or her own property. All employees are responsible for ensuring that the sender of any content to the employee does not violate any copyright laws.

All employees are prohibited from performing all above-mentioned actions, as well as any of the

Following actions:

- Sending, posting or receiving discriminatory, harassing, or threatening messages or images.
- Using the organization's time and resources for personal gain.
- Gambling or playing computer/Internet Games.
- Viewing content of explicit nature, pornography, or any other sexual content, comments, or images.
- Sharing NCHR data with any individual.
- Writing viruses, files, or otherwise tampering with or compromising the security of our computers.
- Sending or posting messages that are disparaging to our organization's image, or the image of any other organization, including their products and services.
- Passing off personal views as those of INTERMEDIA.
- Sending anonymous, bulk, or chain E-mails.
- Copying, pirating, or downloading software and electronic files without permission.
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization.
- Violating copyright law.
- Sending or posting messages that defame or slander other individuals.
- Attempting to break into the computer system of another organization or person.
- Using the Internet for political causes or activities, or religious activities.

Mobile Internet (Edge/Evo):

In emergency situation and environments where internet is unable, NCHR may permit the use of portable internet mobile device, use of portable internet USB device is limited

because they are costly (equipment and volume charges). Selection of appropriate mobile USB service provider is the responsibility of the IT department. As a result, service provider may vary according to different location.

- In most cases, use of mobile internet USB devices will be on temporary bases and is subjected to availability, the operation department is responsible for issuing these devices to staff members (follow the same procedure of equipment issuance) staff member will be responsible for any kind of loss, damage and misuse.
- In environments where internet access is frequently unstable, portable mobile internet USB devices may be assigned to staff members. Only those positions up to manager level are eligible for this allocation, however this does not mean that these devices will be issued to every staff members in the band and above, department heads will be responsible for requesting of portable mobile internet device from the operation department to eligible staff member with in their department.
- Allocation of portable mobile internet USB device on a long-term basis for staff outside of these bands required a clear justifications and recommendations from the department head and approval of the ED.

User Account Management Procedure

a. Upon offer acceptance, the HRD will send the “Joining Report” email for the new employee (or consultant) and send to IT for processing.
b. NCHR will create a secure email account for the staff joining the office.
c. As each staff has allocated a limited Quota on the Server, in order to keep the email account active and avoid interruption in the email communications the outlook will be configured to auto archive the emails after two months period to keep the quota maintained.
d. Use of an official email for correspondence with insecure email accounts (Yahoo) may cause leakage of information as if we send or receive emails from those accounts which are not secure our communication can be interrupted and can be viewed at the ISP or at the country gateway or through any sniffing software.
e. G-mail account with all the security and privacy setting applied are suggested to use for advertisements of jobs, expression of interests, and procurements.

NOTES:

- If a Short-term Employee or Consultant requires an extension, IT Department will only extend the account if notified by the HRD. This cannot come directly from the Department because the employee will also need to be issued a new Agreement / Contract.
- Upon Notification of Transfer, the HRD will send a “transfer” email to IT for processing.
- IT Department will update the user account based on new Profile Type (includes removing old settings).
- Upon Notification of Separation Date, the HRD will initiate a “separation” email and send to IT for processing.
- IT Department will terminate the user account and access levels on the employee’s last day of work and download emails to a PST file.

Handling Exceptions and Urgent Requests

- Due to the nature of NCHR work, there will be cases where urgent requests related to user account management processes will occur, but these should be kept to minimum, and should be the exception not the norm. In such cases, the IT team will try their best to cooperate and respond to such urgent requests. In cases of urgent requests, the Supervisor or Administration Officer should send an urgent message via email to IT Manager.

Use of Official Social Media Accounts

Ownership and Management

The designated team or department inside the commission that is responsible for communications, marketing, or public relations is the one that owns and manages the official social media accounts of the commission.
On the basis of their work duties and areas of expertise, employees may be given access to official social media accounts or allocated individual positions within the commission.

Content Generation and Distribution

Employees who have been granted permission to access official social media accounts are expected to comply to the content rules and approval procedures that have been established.
The content that is provided on official social media platforms need to be accurate,

relevant, and in accordance with the commission’s goal, values, and objectives.

Commission Representation

Employees who are representing the commission on official social media accounts are expected to maintain a professional demeanor and in accordance with the criteria established by the commission for all online platforms.
Maintaining a consistent message, tone, and visual identity across all official social media channels is essential in order to strengthen the awareness and legitimacy of the commission via social media.

Participation and Engagement

Employees are strongly encouraged to interact with followers, react to queries, and take part in discussions on official social media platforms in a way that is both polite and timely.
When dealing with delicate or contentious subjects, it is important to use discretion in order to prevent putting the commission’s image at danger.

Engagement and discourse

Official social media channels should act as venues for creating meaningful discourse, engagement, and cooperation with stakeholders, including civil society groups, government agencies, and the public.
Constructive and courteous talk should be encouraged, but hate speech, harassment, or incitement to violence should be immediately handled and regulated.

Compliance and Security

It is of the utmost importance to ensure total compliance with all applicable regulatory rules, industry standards, and platform policies that regulate the usage of social media. It is essential that precautions be taken in order to protect government social media accounts from being hacked, accessed without authorization, or used inappropriately.

Fact-checking and verification techniques should be implemented to prevent spreading misinformation or disinformation.

Implementation

The selected team or department responsible for official social media accounts will supervise the execution of this policy.
Training sessions and materials should be offered to staff allowed access to

commission’s social media accounts to ensure they understand their duties, responsibilities, and the rules established in this policy brief.

Respect for cultural diversity, religious beliefs, and human dignity should be respected in all statements on government social media platforms.
Regular audits and monitoring of government social media outlets should be done to ensure compliance with the policy and to resolve any problems or concerns quickly.

Data Safety & Privacy and Roll of IT Staff

1. Staff is advised to keep the official data which is need to be backed up in separate location to prevent mixing with unwanted data. The auto backup will be configured only for source locations where there is email archives and official data.
2. Staff are advised to avoid keeping personal data including photos, videos and audios, as if accidently the staff moved their personal files and data in to the specified locations where there is official data, the auto backup software will back up your personal data.
3. Auto Backup will be scheduled weekly bases to avoid maximum loss of precious data, in order to have full and successful implementation of the auto backup system; an orientation on data management will be given to all staff. IT department will schedule the backup plan for all the staff.
4. The auto backup software will encrypt and password protects the backup, in order to make it inaccessible to unauthorized.
5. The backups will be kept offsite and will be updated on monthly bases regularly; the offsite location will be decided by the senior management.
6. Staff is advised not to delete or format the system having official data, as this is property of the Commission
7. At the time of leaving the Commission the equipment issued to the staff will be returned to Operation and after technical verifications and retrieval, changing of all the passwords of email accounts, FTP and computer the exit checklist will be signed for further clearance. The computer received will be cleaned by using the eraser software in order to clean the storage, fresh software installation will be done after cleaning the system storage.
8. All the computers need to have operating system installed in which there is encryption option enabled, windows 7 ultimate, enterprise edition is recommended.
9. For field staff IT department will encrypt as a whole or a portion of the entire hard drive-in order to make the valuable data inaccessible.

10. User account and shared folders on the server will be only accessible to the respective user only; IT department will insure the privacy of those shared folders and users' data.
11. None of the IT staff is allowed to access staff account in any case without the approval of the senior management, or access will be granted to only senior management in case there is need of accessing staff account.
12. Remote access to any user computer is not allowed, remote access will be disabled before issuing a computer system to the staff.
13. In case staff needs remote assistance, after user permits, IT staff will provide remote assistance using team viewer remote assistance tool, this required user's permission to connect remotely.
14. Access to NCHR data base will be provided only to concerned staff after the approval of the Chairperson.
15. The database will be password protected in order to avoid unauthorized access to it.
16. In order to keep the staff aware of the data security and privacy, IT department will plan data
17. A separate internet access will be provided to visitor for the purpose to keep them away from the office network.
18. All website data and login passwords related to website should be shared with ED and Chairman Board of Trustee.

Questions

If you have any question or comments about this IT usage Policy, please contact at ***itadmin@nchr.gov.pk*** . If you do not have any questions, the department of IT & the National Commission for Human Rights presumes that you understand and are aware of the rules and guideline in this IT usage policy and will adhere to them.