CYBER SECURITY POLICY

NATIONAL INSTITUTE OF PLANT GENOME RESEARCH
NEW DELHI - 67

TABLE OF CONTENTS

A. PURPOSE

Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of Information and Communication Technology (ICT) devices and networks. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it. The IT investment of NIPGR is considerable, and our dependency on computing in research work is very high. It is our endeavour to provide all faculty, students and staff with a modern, fully networked computing and IT environment for academic use. It is equally important to ensure cyber security and to prevent targeted cyber-attacks and pilferage of data, as well as effective protection and proper usage of computer systems within the campus. The purpose of this IT usage and support policy is two-fold: to protect the organization/user and to make proper use of computing, networking and IT facilities.

Every organization works within a community or society, and the internet is one of the main ways of communicating with those outside the organization. As such, it is open to misuse which can do substantial damage to the organization. The internet/LAN facility in the Institute has been provided to different users like scientists, staff, students and researchers in office, labs, residences and hostel for use in official/ research purpose. The guidelines/ instructions to streamline the use of this facility are accordingly issued from time to time (Circular 14 File No. NIPGR/19/35/08 dated July 25, 2008; Circular 998 File No. NIPGR/ 19 /35 dated October 09, 2009 and Circular 553 File No. 1-5(2)/15/NIPG/Admn. dated February 27, 2015). By clearly defining what staff can and cannot do with IT assets and equipment, and ensuring that usage of assets is in line with overall ethos of Government of India, staff can feel secure and comfortable in the knowledge they are operating within safe guidelines.

To meet these objectives and in compliance of DO No. 281/27/2/2015-TS dated February 05, 2015 by the Government of India, it has become mandatory to ensure strict compliance of security instructions provided under the National Information security policy issued by the Ministry of Home Affairs and Cyber Security Policy issued by Department of Information Technology. The NIPGR IT usage and support policy has been designed to suit our specific ICT needs and to preserve the utility and flexibility of the system, protect the privacy and work of students and faculty, and preserve our right to access the international networks to which the system is connected.

All concerned are, therefore, advised to abide by the instructions within the policy framework.

B. INTRODUCTION

The IT usage and support policy is an evolving effort towards achieving cyber and data security at the institute and it caters to the whole spectrum of ICT users within NIPGR aiming to serve as an umbrella framework for defining and guiding the actions related to security of our data in cyberspace. This policy will assist in maintaining systems and internet technology at operational level. Contraventions of the Policy could seriously disrupt the operation and any breaches will be treated seriously. Broadly, the policy can be classified in following groups:

1. Network and Data Security Policy
2. Academic Email Support Policy
3. Computational Support Policy

(Detailed usages for each section are explained for its better understanding in the following sections)

C. Implementation and Review

All Lab-in-Charge(s), Scientist-in-Charge(s) of Facilities, Wardens and Manager, will be responsible for the implementation of this policy in their respective areas of responsibility.

Network management, administration and maintenance within NIPGR are the responsibility of Sub-Distributed Information Centre (DISC). The DISC shall be responsible for regular reviewing of policy and to issue from time to time the guidelines based on changes in law or instructions by the Government of India or by NIPGR administration. The Scientist-In-charge DISC (or Director's nominee) will liaise with Administration to ensure adequate cyber security measures. The DISC will ensure that staff is aware of any restrictions and limitations.

In case of complaints, appropriate action to be taken will be decided and taken by the Scientist-in-charge of the facility in consultation with the Administration (Manager) or Director, as appropriate.

D. Cyber Security Awareness

Efforts will be made to develop awareness on challenges of cyber security among NIPGR members.

1. NETWORK AND DATA SECURITY POLICY

This policy includes activation of internet on any computing devices at NIPGR or connected to the NIPGR LAN network using any connection method. This includes but not limited to following items:

1. Desktop Computer systems, Servers and Workstations
2. Printers & Scanners, Laptops, Palm tops
3. Switches, Modem, Routers, and Firewall
4. Scientific Research Equipment
5. UPS systems, Floppies, CDs, DVDs, Blue tooth, Pen Drives, Detachable hard disk, CD/DVD writers etc.

1.1. Main Aspects of Policy

1. Access to main servers will be restricted to authorised staff only.
2. All devices owned by the organization or allowed on the organization network must be registered by their MAC/IP address to the DISC before being connected. Each device user must be identified by name and information must be given to the DISC. Upon enrolment, DISC shall issue an IP-specific USERNAME and PASSWORD to avoid IP misuse.
3. All computers requiring access must be pre-loaded with anti-virus program and latest possible virus updates. Any data stored on computers other than the server shall be the responsibility of the concerned user in terms of safety and backup.
4. All Lab-in-Charge(s), Scientist-in-Charge(s) of Facilities, Wardens and Manager must ensure that unauthorized persons cannot gain access to the computers within their domain. No software or application shall be loaded without proper licenses to avoid security problem on the network by installing and running an unapproved program
5. Every lab can have a maximum of seven activated IPs at a given time. These will be provided on registered institutional devices listed above.
6. Temporary staff will not be provided internet on their personal devices.
7. Each Guest house, hostel room and residential quarter unit will have one dedicated IP.

1.1.1 Internet Access Form

To keep a further check on the effective usage of the internet, every individual requiring internet must forward the request of internet activation/access by the scientist/officer/student/researcher in the prescribed INTERNET ACCESS FORM (Annexure I) duly recommended by the concerned In-charge, as given below:

Staff Members	:	Lab-In-charge / Manager / Scientist-In-charge
Students/Hostellers	:	Supervisor and Warden
Scientists	:	Director or his authorized person

1.1.2. Internet Support

An inventory of IP activated computing equipment will be maintained by the DISC to ensure full tracking of equipment, along with details of the security configuration and related licenses. Problems with network/software/Internet should be reported to the DISC in accordance with established Help Desk procedures. An online helpdesk is available at http://nipgr.res.in/helpdesk.html for any kind of assistance required with internet at the institute. Offline complaints shall be entertained through duly filled COMPLAINT FORM available with DISC and NIPGR web page (http://nipgr.res.in/misc/forms.php) (Annexure II).

1.2. Internet Usage Guidelines

1. Faculty, staff, and students with authorized accounts may use the computing and IT facilities for academic purposes, official Institute business, and for personal purposes so long as such use:
   a. Does not violate any law, Institute policy or IT act of the Government of India.
   b. Does not interfere with the performance of Institute duties or work of an academic nature (as judged by the respective in-charges).
   c. Does not result in commercial gain or private profit other than that allowed by the Institute.

1.2.1. Cyber-security policy pertaining to all working areas

1. Any attempt to circumvent system security, guess others’ passwords, or in any way gain unauthorized access to local or network resources is forbidden. Users may not use another person's computing account, attempt to forge an account identity, or use a false account or e-mail address. No user is allowed to alter internet browser settings.

2. Transferring copyrighted materials to or from the NIPGR systems without express consent of the concerned in-charge is a violation of international law.

3. Downloading and installing of new software has to be done with the explicit consent of the respective facility in-charges. Facility in-charges should have a record of software installed in the systems present in their laboratories.

4. Recreational downloads and peer-to-peer connections for recreational purposes are banned.

5. No food or drink is permitted in the areas with computing devices. Smoking is strictly prohibited. Also making noise either through games/ music or even talking and/ or singing loudly is prohibited.

6. Display of offensive material (either on computer screens or through posters etc.) is strictly disallowed and serious action will be taken against offenders.

7. Access to non-official websites such as online gaming, business, stock-trading and sites based on religion, gender or political belief, etc. would be considered inappropriate and therefore not allowed.

8. Lab-in-Charge(s), Scientist-in-Charge(s) of Facilities, Wardens and Manager, can frame usage norms for their respective domains, if they consider it necessary. This may include data upload/download limits, additional browsing filters, access time restrictions etc.

9. Any request for remote access using either dial-in, VPN, or any other remote access to the NIPGR network must be reviewed and approved by the concerned in-charge, followed by DISC In-Charge and Director, NIPGR. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

10. The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the new/email groups.

1.2.2. Cyber-security policy pertaining to Library

1. Transferring copyrighted material to and from NIPGR network without consent of the owner (publisher) is a violation.
2. Copyrighted e-resources such as e-journals, e-books, databases, etc. made available by NIPGR are for academic use only.
3. By using NIPGR IT infrastructure, these resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material.
4. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited.
5. Use of robots, spiders or intelligent agents to access, search and/or systematically download from e-resources is also prohibited.

1.2.3. Relaxation to Guidelines

1. New scientists can use up to two IPs on personal devices till official procurement of computing equipment is completed, or 1.5 years, whichever is earlier.
2. For requirement of more than seven IPs, a detailed justification for each additional IP must be provided, increase in number of staff will not be considered sufficient justification.
3. Third parties like software developers from the company/ external organization often require internet usage to connect their laptop to NIPGR LAN for short duration. Such cases as far as possible be restricted or be allowed on case to case basis after ensuring absolute caution. The third party request should be forwarded by the respective In-charge on the duly filled in INTERNET ACCESS FORM (Annexure – I).
4. Notwithstanding contained anything in this policy, Director NIPGR will be the final authority regarding relaxation and interpretation of any clause contained herein.

1.2.4. Safety-related Suggestions

1. All computers must be password protected and only System administrator/HOD other than the user should know this account and password.
2. Users are expected to respect the privacy of other users and they may not allow any other person to use their password or share their account.
3. Software installed for doing various activities must have separate user account and password for each user for protection of software and data.

No Dues: Upon tenure completion, following no dues may be submitted to the DISC:

1. Any cables for IP (hostel/ residence)
2. IP address surrender
3. De-registration of internet activated device
4. Email ID cancellation (Grace period: Max 6 months upon written request before end of tenure)

1.3. Wi-Fi Access (Pending Installation of Central Authentication WAPs)

Setting up of unsecured Wi-Fi systems on the NIPGR network is prohibited in accordance with a Government of India ban - Installation of unprotected Wi-Fi routers is banned by a GOI regulation. This GOI regulation prohibits shared access of Wi-Fi resources and mandates Wi-Fi access only through a central authentication mechanism. In view of this, 802.1x (WPA2-Enterprise) is the minimum acceptable standard for setting up Wi-Fi access in the academic area.

Installation of Wi-Fi routers in the academic area will not be permitted without explicit consent from DISC. All users should use the authorized central NIPGR Wi-Fi SSIDs for Wi-Fi access and verify the authenticity of the Wi-Fi routers using the digital certificate duly signed by the DISC.

All Wi-Fi routers that provide connection to the NIPGR LAN should have at least WPA2-PSK (pre-shared key with WPA2 encryption) standard security enabled.

2. ACADEMIC EMAIL SUPPORT POLICY

The academic email domain servers of the institute (NIPGR.AC.IN and NIPGR.RES.IN) have been registered with the NIC, and are assets that can be monitored for usage and data transfer.

An EMAIL ACCESS FORM (Annexure III) may be filled for acquiring academic email account, duly recommended by the concerned In-charge, as given below:

Staff Members	:	Lab-In-charge / Manager / Scientist-In-charge
Students/Hostellers	:	Supervisor and Warden
Scientists	:	Director or his authorized person

Email support and access will be provided and maintained by the DISC. Presently, following emailing groups are available at the institute:

1. faculty@nipgr.ac.in (All faculty members of the Institute)
2. alladmin@nipgr.ac.in (All admin, finance, engineering staff of the Institute)
3. technical@nipgr.ac.in (All technical staff of the Institute)
4. students@nipgr.ac.in (All PhD students of the Institute)
5. researchers@nipgr.ac.in (All students & researchers includes RAs, JRFs, SRFs, TAs etc.)
6. allusers@nipgr.ac.in (Includes all above users from Sr. No.1 to 5)

2.1. Main Aspects of Policy

1. NIPGR academic email ID will be provided only to institutional staff members, researchers and students in the form of userame@nipgr.ac.in
2. The email facility will be withdrawn upon resignation or tenure completion of the concerned individual
3. To the extent possible, users are expected to use only their official email addresses provided by NIPGR for official communications with other members of the Institute.
4. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data.

5. It is also forbidden to send emails or messages masquerading as another person or to hide the sender's identity. Chain letters are not allowed. Neither is any form of commercial advertising, or soliciting allowed.
6. Spamming is strictly disallowed. Subscribing to mailing lists outside the Institute is an individual’s responsibility. Subscribing someone else to any group outside NIPGR is illegal.
7. Users are forbidden to send frivolous or academically unimportant messages to any group. Broadcast of messages to everyone in the system is allowed only for academic purposes and emergencies. Violations of this (as decided by concerned authorities) will result in immediate freezing of user's account for an extended period as determined by the authorities.
8. Shared email accounts for any purpose whatsoever are not allowed.
9. Any special accounts, if need to be set up for conferences and other valid reasons as determined by the institute authorities, must have a single designated user.
10. The email facility provided to staff should not be used for political, business or commercial purpose not related to the organization.
11. Staff should minimize the number of messages in their inbox to ensure maximum efficiency of the delivery system.
12. NIPGR retains the right to monitor any or all emails sent and received by the academic servers.

3. COMPUTATIONAL SUPPORT POLICY

Informatics encompasses the use of computational, mathematical and statistical methods to organize, analyze and interpret information. Bioinformatics deals with these aspects, particularly at the molecular, genetic and genomic levels.

Bioinformatics is central to the interpretation and exploitation of the wealth of plant biological data being generated in the post-genome era, leading to application oriented benefits in agriculture and pharmacology.

Since a major part of NIPGR research work relies on Bioinformatics, support can be provided in a variety of ways to assist researchers and scientific groups in their work, depending upon the expertise available.

3.1. Main Aspects of Policy

1. Online databases and web-servers may be hosted on the NIPGR main web server, depending upon availability and feasibility. All such requests should be made to the DISC-In-Charge.
2. Guidelines for shared usage of High Performance Computing Facility (HPC) will be formulated and distributed from time to time for users.
3. Programming support will be provided to scientists and staff for general programming related tasks in day to day institutional work.
4. It may be noted that Data Storage support cannot be provided in any form, and all kinds of data storage and backup must be carried out within the respective domains.
5. Computational Support Facility (CSF) at the institute can be requested in case any staff member or researcher requires support with programming.
6. A CSF SUPPORT INDENT (Annexure IV) may be filled for programming related work, duly recommended by the concerned In-charge, as given below:

Staff Members	:	Director / Manager /Lab. or Scientist-In-charge
Students	:	Supervisor

This form should be signed by the indentor authorized by the Competent authority and countersigned by CSF-in-Charge before submission to the CSF staff for processing and work completion.

3.2. Cyber Security Risk Evaluation

The DISC will prepare a list all network security risks and help the administration determine where the greatest threats lie on the network. This may include an opinion of the severity of each threat and how common it is on the network, and the rate at which this threat has materialized. There are several main items to consider when listing threats and their ability to threaten the network, such as:

1. Threats such as virus, spyware, worms, computer hack and others. Hostile software through email borne viruses into user computers & servers. Threats to server from user computers.
2. Unauthorized user installed programs - Users bringing their own programs into the network on disks or memory sticks; Lab-in-Charge(s), Scientist-in-Charge(s) of Facilities, Wardens and Manager must ensure protection against this in their domains.
3. Attacks to the server through vulnerable applications, or through vulnerabilities in services such as web server and mail services, operating systems or wrong configuration of services.

3.3. Cyber Security and Support Policy Documentation

The network structure and configuration shall be documented by DISC and they will maintain the following information:

1. IP addresses of all devices on the network with static IP addresses.
2. Network drawings with locations and IP addresses of all hubs, switches, modems, routers, and firewalls on the network, various security zones and devices that control access between them. The interrelationship between all network devices showing lines running between the network devices, subnets on the network, their IP range and net mask information.
3. Configuration information on all network devices. Configuration shall include but not be limited to IP Address, MAC address, Netmask, Default gateway, DNS server IP addresses for primary and secondary DNS servers, and any relevant server information.

4. Network documentation shall be kept either in written form or electronic form, preferably in two places, spatially apart so that if one facility is destroyed, information from the other facility may be used to help re-construct the IT infrastructure. Only authorized institutional staff shall have full access to all network documentation.

3.4. Contravention of the Policy

All members of NIPGR should be aware of their responsibilities under the Data protection Act, Computer Misuse Act and the Copyright Design and Patents Act by Govt. of India.

Contravention of the NIPGR IT usage policy or any act of deliberate sabotage to NIPGR computer devices and networking equipment shall be considered a serious offence and will be dealt severally subject to disciplinary action.

Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the institute may take action by issuing a warning through disabling the account. In extreme cases, the account may be completely deleted and/ or the user prohibited access to IT facilities at NIPGR, and/ or sent to the Institute disciplinary action committee as constituted by the Institute authorities. Violations of email policy guidelines can result in immediate freezing of user's account for an extended period as determined by the authorities.

3.5. Network Access and Monitoring

NIPGR is required by GOI guidelines to be able to associate every internet access using its facilities to specific users and maintain logs of all such accesses. NIPGR reserves the right to monitor any and all of its IT facilities to determine if a user is acting unlawfully or violating this policy or any other policy or rule. Such monitoring may include, individual login sessions, the Internet sites visited by users and the content of electronic communications. Monitoring may be done with or without prior notice to the user.

Internet Access Form (NIPGR) Annexure I

User Name:
Designation:
Laboratory:
Date:
Validity Period:
Contact No.:

Connection Type:	□ **LAN** □ **Wi-Fi**	**Lab No./Location:**	
Device Type:	**PC / LAPTOP / MOBILE**	**No of Active Connection:**	

Information Required

MAC ADD. :	**ANTIVIRUS :**
O. SYSTEM :	**ANTIVIRUS STATUS :**
DLP Installation Status:	

Note: The usage is subject to the understanding that the user is aware of Internet anti-abuse measures generally and is willing to adhere to them. By logging in, the user agrees to accept liabilities of all kinds that may arise from any measure of deemed abuse in standard parlance in cyber-law matters.

Recommending Officer:		**Reason for Wi-Fi Connection:** (In case of Ph.D. Students and Project Fellows)
Signature:		
Name:		
Designation		
DISC Authorization:		**Remarks (If Any)**
Signature:		
Name:		
Designation		

Declaration: I have read and understood the NIPGR Cyber Security Guidelines and agree to abide by the policies and instructions contained therein.

User Signature

For DISC Use

Internet Access enabled by: ______________ Enabled on: ___________

INTERNET ACCESS DETAILS

IP NUMBER: **Y** □ **N** □
USERNAME AUTHENTICATION ENABLED: **Y** □ **N** □
USER GROUP DETAILS:
PREVIOUS IP ALLOTTED, IF ANY:

*** Only fully filled form will be accepted. Incomplete Forms will not be accepted.**
*** Internet facility will not be provided on Personal Devices of temporary staff.**

राष्ट्रीय पादप जीनोम अनुसंधान संस्थान

NATIONAL INSTITUTE OF PLANT GENOME RESEARCH

Requisition for Institutional Official Email ID

Personal Information			
Name in full (Block Letters) :			
Job Title :			
Name/ Dept. Head :			
Lab / Department :			
Joining Date :		**Tenure Upto*:**	
Contact No. :			
User Information			
Type for Issue :	**Create New :** □	**Reactivate :** □	
USER ID :	*Choice 1.* *Choice 2.*		@nipgr.ac.in @nipgr.ac.in
Reason for Issue :			
Other Existing Email Address	*1.* *2.*		

Note: Access to the academic email system is provided for scientific purposes only and this facility cannot be used to send illegal or inappropriate material, or for political, business or commercial purpose not related to NIPGR. Institute retains the right to monitor any or all emails sent and received by the academic server.

Recommending Officer's Signature ***User Signature***

DISC Authorization

Dr. Jitendra K. Thakur, Scientist-in-Charge, DISC Facility

Signature ……………………………………..

For DISC Use

Email ID Provided :

Date of Activation : ***Valid Upto :***

Signature (DISC Staff)

- *Incomplete Forms will not be considered.*
- *Official Email account must be surrendered by user upon tenure completion*
- **The provided Email ID would be extendable based on Email request to DISC*
- *Email ID and Password should have minimum of six characters – Please do not share with anyone*

NATIONAL INSTITUTE OF PLANT GENOME RESEARCH

SUPPORT CENTER

Welcome to NIPGR Support Center

BACK

Name: ______ Scientist ▼

LAB/ Dept. : ______

Contact No. : ______

Email ID : ______ [example@nipgr.ac.in]

ISSUE Related : **Internet** ○ **Others** ●

Details - ______

Computer Location : ______

Submit Complaint Reset

Distributed Information Sub-Center

Annexure IV

NATIONAL INSTITUTE OF PLANT GENOME RESEARCH
COMPUTER SUPPORT FACILITY (CSF)
INDENT FORM

Date: …………………

Name : ______________________________

Contact telephone/Mobile no. : ______________________________

Lab or Scientist Incharge/Manager/Director : ______________________________

Programming Work Requirement in relation to **(Tick appropriate box √)**

1. Web Design □
   (Java, CGI, CSS, PHP, HTML, others)
2. Data Analysis □
3. Database □
   (MySQL, Oracle, DB2, SQL, others)
4. Others □

Specifications : ______________________________

____

____

____

____

Signature of Indentor	Lab or Scientist Incharge/Manager/Director	Scientist-in-charge (CSF)
Date:	Date:	Date:

(For CSF Use Only)

Date of Indent received :

Tentative Time Required :

Date of Completion :

Remarks :

Technical Staff	Scientist In-charge
Date:	Date: