



NAVSARI AGRICULTURAL UNIVERSITY

શ્રી સી. બી. નાયક
હિસાબ નિયામક અને નિયંત્રણ
અધિકારી (આઈ.ટી.)

હિસાબ નિયામકશ્રીની કચેરી

ઇન્ફોર્મેશન ટેકનોલોજી વિભાગ

નવસારી કૃષિ યુનિવર્સિટી, નવસારી
યુનિવર્સિટી ભવન, એડુ ચાર રસ્તા, દાંડી રોડ, નવસારી - ૩૮૬૪૫૦
✉ ઇ-મેઇલ: itcell@nau.in ☎ ફોન: (મો): ૭૩૫૮૪૪૫૫૪૪



ખાસ અગત્યનું

વિષય:- સાયબર સિક્યોરીટી ગાઈડલાઈનના અમલીકરણ અંગે.

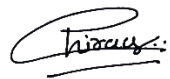
- વંચાણે લીધા :-**
- ૧.) નાયબ સચિવ (આઈ. ટી.), કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ, ગુજરાત રાજ્ય, સચિવાલય, ગાંધીનગરના પત્ર : File No: ACD/CIO/e-file/2/2023/0457/IT Section
 - ૨.) નવસારી કૃષિ યુનિવર્સિટીના આઈ.ટી સેવાઓના અમલીકરણ અંગેનું તા. ૦૧/૦૮/૨૦૧૮ના રોજનું જાહેરનામું નં. ૬૪૮/૨૦૧૮.

ૐ પરિપત્ર ૐ

આથી અત્રેની યુનિવર્સિટીના તમામ (કાયમી/હંગામી/આઉટસોર્સ) અધિકારીશ્રીઓ/કર્મચારીશ્રીઓ ને જણાવવાનું કે, રોજબરોજના ઓફીસ કાર્યોમાં ટેકનોલોજી અને ઇન્ટરનેટના વધતા ઉપયોગ સાથે મજબૂત સાયબર સુરક્ષા પગલાંની જરૂરિયાત નિર્ણાયક બની ગઈ છે. જે પુરતી તકેદારી ન રાખવામાં આવે તો સાયબર હુમલાના ગંભીર પરિણામો આવી શકે છે. જેમાં નાણાકીય નુકસાન, પ્રતિષ્ઠાનું નુકસાન અને વ્યક્તિગત માહિતી સાથે છેડાનો સમાવેશ થાય છે. સામેલ સૂચિત સાયબર સિક્યોરીટી ગાઈડલાઈનનો અમલ કરવાથી સાયબર હુમલાઓને રોકવામાં, ડેટા ચોરી અને વાયરસ સામે રક્ષણ કરવામાં મદદ મળી શકે છે. જેથી નાયબ સચિવ(આઈ. ટી.), કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ, ગુજરાત રાજ્ય, સચિવાલય, ગાંધીનગરના ના ઉક્ત વંચાણે લીધેલ ક્રમ-૧ ના પત્ર તેમજ નવસારી કૃષિ યુનિવર્સિટીના ક્રમ-૨ ના આઈ.ટી સેવાઓના અમલીકરણ અંગેના જાહેરનામા અન્વયે નવસારી કૃષિ યુનિવર્સિટીમાં સાયબર સિક્યોરીટી ગાઈડલાઈનનો ચુસ્તપણે અમલ કરવા જણાવવામાં આવે છે.

બીડાણ : વંચાણે લીધેલ સદર્ભ પત્ર - ૧ અને ૨.

ખ.નં. નક્યુ/હિનિ/આઈ.ટી./ટી-૫/૩૮/૨૦૨૩
નવસારી, તા. ૧૭/૦૨/૨૦૨૩


હિસાબ નિયામક અને નિયંત્રણ
અધિકારી (આઈ.ટી.)

નકલ સવિનય રવાના (e-પરિપત્ર વ્હારા):-

તમામ યુનિવર્સિટી અધિકારીશ્રીઓ તરફ આપશ્રીની તાબા હેઠળની કચેરીઓ તરફ અમલ કરાવવા સારૂ.

નકલ રવાના (e-પરિપત્ર વ્હારા):-

યુનિવર્સિટીના તમામ યુનિટ / સબ યુનિટના વડાશ્રીઓ તરફ જણ તથા અમલ થવા સારૂ.



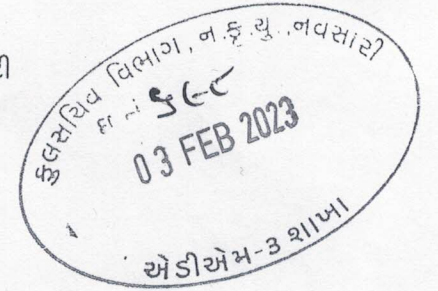
આઈ.ટી. શાખા

કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ

સચિવાલય, ગાંધીનગર.

પ્રતિ,

- (૧) ખેતી નિયામકશ્રી, ખેતી નિયામકશ્રીની કચેરી, ગુજરાત રાજ્ય, કૃષિ ભવન, ગાંધીનગર.
- (૨) બાગાયત નિયામકશ્રી, બાગાયત નિયામકશ્રીની કચેરી, ગુજરાત રાજ્ય, કૃષિ ભવન, ગાંધીનગર.
- (૩) પશુપાલન નિયામકશ્રી, પશુપાલન નિયામકશ્રીની કચેરી, ગુજરાત રાજ્ય, કૃષિ ભવન, ગાંધીનગર.
- (૪) મત્સ્યોદ્યોગ કમિશ્નરશ્રી, મત્સ્યોદ્યોગ કમિશ્નરશ્રીની કચેરી, ગુજરાત રાજ્ય, ડૉ.જીવરાજ મહેતા ભવન, ગાંધીનગર.
- (૫) રજિસ્ટ્રારશ્રી, સહકારી મંડળીઓ, ગુજરાત રાજ્ય, ડૉ.જીવરાજ મહેતા ભવન, ગાંધીનગર.
- (૬) ખાંડ નિયામકશ્રી, ખાંડ નિયામક ઓફિસ, ગુજરાત રાજ્ય, ડૉ. જીવરાજ મહેતા ભવન, ગાંધીનગર.
- (૭) મુખ્ય કારોબારી અધિકારીશ્રી, ગુજરાત લાઈવ સ્ટોક ડેવલપમેન્ટ બોર્ડ, બ્લોક-એ, ગુજરાત રાજ્ય, કૃષિ ભવન, ગાંધીનગર.
- (૮) નિયામકશ્રી, ખેત બજાર અને ગ્રામ્ય અર્થતંત્ર, ગુજરાત રાજ્ય, ડૉ.જીવરાજ મહેતા ભવન, ગાંધીનગર.
- (૯) મુખ્ય કાર્યપાલક અધિકારીશ્રી, નિરીક્ષણ અને અન્વેષણ સમિતિ, એ-વિંગ, બાજો માળ, બહુમાળી ભવન-૨, વસ્ત્રાપુર, અમદાવાદ.
- (૧૦) રજિસ્ટ્રારશ્રી, ગુજરાત રાજ્ય સહકારી ટ્રીબ્યુનલ, સહકારી બહુમાળી મકાન, લાલ દરવાજા, અમદાવાદ.
- (૧૧) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત રાજ્ય બીજ પ્રમાણન એજન્સી, 'બીજ પ્રમાણન ભવન', શ્યામલ રો-હાઉસ, વિભાગ-૫ બસ સ્ટેન્ડ પાસે, ગોકુલ રો-હાઉસ સામે, અમદાવાદ.
- (૧૨) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત રાજ્ય વેરહાઉસીંગ કોર્પોરેશન, કર્મચોગી ભવનની સામે, સેક્ટર-૧૦-એ, ગાંધીનગર.
- (૧૩) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત રાજ્ય ઘેટાં અને ઊન વિકાસ નિગમ લિમિટેડ, ઉદ્યોગ ભવન, સેક્ટર-૧૧, ગાંધીનગર.
- (૧૪) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત મત્સ્યોદ્યોગ કેન્દ્રીય સહકારી સંસ્થા લિમિટેડ, સાકાર-૭, ભોંયરુ, એસ-૨ થી એસ-૪, નહેરુ બ્રિજ કોર્નર, આશ્રમ રોડ, અમદાવાદ.
- (૧૫) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત રાજ્ય કૃષિ બજાર બોર્ડ, ગુજરાત રાજ્ય, ડૉ. જીવરાજ મહેતા ભવન, ગાંધીનગર.
- (૧૬) સભ્ય સચિવ સહ સંયુક્ત પશુપાલન નિયામકશ્રી, ગૌસેવા અને ગૌચર વિકાસ બોર્ડ, ગુજરાત રાજ્ય, ડૉ. જીવરાજ મહેતા ભવન, ગાંધીનગર.
- (૧૭) નિયામકશ્રી આત્મા, સેક્ટર-૧૦-એ, કૃષિ ભવન, ગાંધીનગર.
- (૧૮) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત ખેત ઉદ્યોગ નિગમ, ગુજરાત રાજ્ય અન્ન પુરવઠા નિગમનું વહીવટી સંકુલ, સેક્ટર-૧૦એ, ગાંધીનગર.
- (૧૯) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત રાજ્ય જમીન વિકાસ નિગમ, બલરામ ભવન, ગાંધીનગર.
- (૨૦) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત રાજ્ય બીજ નિગમ, સેક્ટર-૧૦એ, ગાંધીનગર.
- (૨૧) મેનેજીંગ ડિરેક્ટરશ્રી, ગુજરાત ડેરી વિકાસ નિગમ લિમિટેડ, સેક્ટર-૧૬, ગાંધીનગર.
- (૨૨) નિયામકશ્રી, ગુજરાત ઓર્ગેનિક પ્રોડક્ટસ સર્ટીફિકેશન એજન્સી(GOPCA), બીજ પ્રમાણન ભવન, શ્યામલ ચાર રસ્તા, ગોકુલ રો હાઉસ સામે, સેટેલાઈટ, અમદાવાદ.
- (૨૩) રજિસ્ટ્રાર, ગુજરાત ઓર્ગેનિક કૃષિ યુનિવર્સિટી, આણંદ કેમ્પસ, આણંદ.
- (૨૪) સંયુક્ત પશુપાલન નિયામકશ્રી, ગુજરાત રાજ્ય પ્રાણી કલ્યાણ બોર્ડ, સુમન ટાવર, બીજો માળ, સેક્ટર-૧૧, ગાંધીનગર.
- (૨૫) રજિસ્ટ્રાર, કામધેનુ યુનિવર્સિટી, બ્લોક-૧, બી-૧ વિંગ, ચોથો માળ, કર્મચોગી ભવન, ગાંધીનગર.



Signature Not Verified
Signed by: ANITA P ZULA
Date: 2023/02/25
53:59 +05:30

File No: ACD/CIO/e-file/2/2023/0475/IT Section

Approved By: ANITA P ZULA(DS,IT Section,ACD)

Open the document in Adobe Acrobat DC to verify the E-sign



02 FEB 2023

PSR/IT Cell
PSR/IT Cell
Vge

In W.No.....34

Date.....04-02-23

I.T., N.A.U., NAVSARI.

(૨૬) રજિસ્ટ્રાર, આણંદ કૃષિ યુનિવર્સિટી, યુનિવર્સિટી ભવન, આણંદ.

(૨૭) રજિસ્ટ્રાર, નવસારી કૃષિ યુનિવર્સિટી, એર ચાર રસ્તા, દાંડી રોડ, નવસારી.

(૨૮) રજિસ્ટ્રાર, જૂનાગઢ કૃષિ યુનિવર્સિટી, યુનિવર્સિટી ભવન, જૂનાગઢ.

(૨૯) રજિસ્ટ્રાર, સરદાર કૃષિનગર દાંતીવાડા કૃષિ યુનિવર્સિટી, સરદાર કૃષિનગર, બનાસકાંઠા.

(૩૦) સહ પ્રાધ્યાપક, રાજ્ય કૃષિ યુનિવર્સિટી પરિષદ, પોડીયમ લેવલ, કૃષિ ભવન, ગાંધીનગર.

(૩૧) રજિસ્ટ્રાર, ગુજરાત વેટરનરી કાઉન્સિલ, બ્લોક નં.: ૧૪/૧, જીવરાજ મહેતા ભવન, ગાંધીનગર.

(૩૨) નાયબ સચિવ/ઉપસચિવ/સેક્શન અધિકારી (તમામ), કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ, સચિવાલય, ગાંધીનગર.

વિષય: સાયબર સિક્યોરીટી ગાર્ડલાઈનના અમલીકરણ અંગે

શ્રીમાન,

સવિનય ઉપરોક્ત વિષય અન્વયે જણાવવાનું કે રાજ્ય સરકાર ની સેવાઓમાં ટેકનોલોજી અને ઈન્ટરનેટના વધતા ઉપયોગ સાથે મજબૂત સાયબર સુરક્ષા પગલાંની જરૂરિયાત નિર્ણાયક બની ગઈ છે. સાયબર હુમલાના ગંભીર પરિણામો આવી શકે છે, જેમાં નાણાકીય નુકસાન, પ્રતિષ્ઠાનું નુકસાન અને વ્યક્તિગત માહિતી સાથે ચેડાનો સમાવેશ થાય છે. સૂચિત સાયબર સિક્યોરીટી ગાર્ડલાઈનનો અમલ કરવાથી સાયબર હુમલાઓને રોકવામાં, ડેટા ચોરી અને વાયરસ સામે રક્ષણ કરવામાં મદદ મળી શકે છે. આથી, આપની કચેરી/શાખા તથા આપના તાબા હેઠળની કચેરીઓમાં સાયબર સિક્યોરીટી ગાર્ડલાઈનની સૂચનાઓ ચૂસ્તપણે અમલ કરવા વિનંતી છે.

આપની વિશ્વાસુ,

(અનિતા ઝુલા)

નાયબ સચિવ (આઈ.ટી.)

બિડાણ: સાયબર સિક્યોરીટી ગાર્ડલાઈન

કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ

નકલ રવાના:

- અધિક મુખ્ય સચિવશ્રી(કૃષિ)ના રહસ્ય સચિવશ્રી, કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ, સચિવાલય, ગાંધીનગર.
- સચિવશ્રી(સહકાર, પશુપાલન, ગૌ સંવર્ધન, મત્સ્યોદ્યોગ)ના રહસ્ય સચિવશ્રી, કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ, સચિવાલય, ગાંધીનગર.
- મદદનીશ નિયામકશ્રી (આઈ.ટી.), કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ, સચિવાલય, ગાંધીનગર.
- સિસ્ટમ મેનેજરશ્રી, કૃષિ, ખેડૂત કલ્યાણ અને સહકાર વિભાગ, સચિવાલય, ગાંધીનગર.
- સિલેક્ટ ફાઈલ-૨૦૨૩.



Cyber Security Guideline

DESKTOP/LAPTOP SECURITY

1. Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work. Admin access to be given to users with approval from appropriate authority.
2. Ensure that the Operating System and BIOS firmware are updated with the latest updates/patches.
3. Install Antivirus client/software provided by DST from URL <http://gswan.gujarat.gov.in/> on your systems and ensure that it is updated with the latest virus definitions, signatures and patches.
4. Applications/software's, which are related to official work, shall be installed/used; any other application/software shall not be installed/used.
5. Desktop must be locked/logged off when workspace is unoccupied and must be shut down if not in use.
6. Enable Desktop Firewall for controlling information access.
7. Use VPN service provided by GSDC for connecting to any IT Assets located in State Data Centre and the system must be equipped with up-to-date antivirus software
8. Do not use any external Mobile App based scanner services (ex: Cam scanner) for scanning internal government documents.
9. Don't use pirated Operating systems and software/applications.

INTERNET BROWSING SECURITY

1. While accessing Government applications/services, email services or banking/payment related services or any other important application/services, always use Private Browsing/Incognito Mode in your browser.
2. While accessing sites where user login is required, always type the site's domain name/URL, manually on the browser's address bar, rather than clicking on any link.
3. Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
4. Don't store any usernames and passwords on the internet browser.
5. Don't store any payment related information on the internet browser.
6. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies etc).

7. Don't use any 3rd party toolbars & extensions/plugins (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.
8. Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software's).
9. Don't use your official systems for installing or playing any Games.
10. Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/) or popup window. Many malwares and phishing sites abuse URL shortened services. Such links may lead to a phishing/malware webpage, which could compromise your device.

PASSWORD MANAGEMENT

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
2. Use Multi-Factor Authentication, wherever available.
3. Users must use a separate, unique password for each of their work related accounts.
4. Don't save passwords in the browser or in any unprotected documents.
5. Passwords must be kept secret and should not be shared.

REMOVABLE MEDIA SECURITY

1. Perform a low format of the removable media before the first-time usage.
2. Perform a secure wipe to delete the contents of the removable media.
3. Scan the removable media with Antivirus software before accessing it.
4. Always protect your documents with strong password.
5. Don't plug-in the removable media on any unauthorized devices.

EMAIL SECURITY

1. Do not share the email password with any persons.
2. Don't use any unauthorized/external email services for official communication.
3. Don't click/open any link or attachment contained in mails sent by unknown sender.
4. Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Observe caution with documents containing macros while downloaded as attachments or received from non trusted source, always select the "disable macros" option and ensure that protected mode is enabled on your office productivity applications like MS Office.
5. Disable automatically forwarding email to a third party email system.
6. Do not use official email id provided by Government for any personal usage.

ANTIVIRUS USAGE

1. User shall install enterprise grade endpoint antivirus solution of DST.
2. User can download the antivirus solution from <https://gswan.gujarat.gov.in/>

3. User shall periodically run full scan on his/her computer using above antivirus.
4. User shall uninstall any other antivirus software installed on their system apart from above antivirus solution.
5. Users shall exercise due caution while opening e-mail attachments received from unknown senders as they may contain viruses or other malicious software.
6. User/Department should remove infected device (any virus/malware/ransomware etc.) from GSWAN/Government network and send the report of such device to GSDC Security team at incident-certg@gujarat.gov.in
7. Department/HoD shall ensure that computer systems owned by department shall be kept up to date with latest/supported versions of software and operating system and Anti-virus solution installed.
8. Please refer to Security & Antivirus software guideline at <https://gswan.gujarat.gov.in>

વિષય: એન.એ.યુ. આઈ.ટી. પોલીસીની મંજૂરી અંગે


જાહેરનામું નં. ૬૪૫/૨૦૧૮

આથી સબંધકર્તા સર્વેને જણાવવામાં આવે છે કે, તા. ૫-૭-૨૦૧૮ ના રોજ નવસારી ખાતે મળેલ સંચાલક મંડળની ૪૦મી બેઠકની કાર્યનોંધના મુદ્દા નં. ૪૦.૦૩ થી નીચેની વિગતે ઠરાવ કરેલ છે.

"આથી ઠરાવ કરવામાં આવે છે કે, નવસારી કૃષિ યુનીવર્સિટીમાં આઈ.ટી. સેવાઓના અમલીકરણ માટે નવસારી કૃષિ યુનીવર્સિટી આઈટી પોલીસી Appendix-40.03(i)to(x) મંજૂર કરી કાર્યવન્તીત કરવા માટે પરવાનગી આપવામાં આવે છે."

જા.નં.ન.કૃ.યુ./આઈટી/૧૬૪/૨૦૧૮

તા. ૦૧/૦૮/૨૦૧૮


નિયામક
ઈન્ફોર્મેશન ટેકનોલોજી
નવસારી કૃષિ યુનિવર્સિટી
નવસારી - ૩૮૬ ૪૫૦.

નકલ સવિનય રવાના:

- (૧) સંચાલક મંડળના તમામ સભ્યશ્રીઓ તરફ
- (૨) યુનીવર્સિટીના તમામ અધિકારીશ્રીઓ તરફ
- (૩) તમામ યુનિટ/સબ યુનિટ અધિકારીશ્રીઓ તરફ
- (૪) કુલસચિવ વિભાગની બોર્ડ ઓફ મેનેજમેંટ શાખા તરફ (૦૫ નકલમાં)
- (૫) રહસ્ય સચીવશ્રી [માન. કુલપતિશ્રી/કુલસચિવશ્રી] તરફ
- (૬) જાહેરનામાં ફાઈલ



Policy of Information Technology Resources and Services of NAU – 2017

Abbreviation

- NAU – Navsari Agricultural University
- IT – Information Technology
- UTP - Unshielded Twisted Pair
- VPN – Virtual Private Network
- ERP – Enterprise Resource Planning
- NOC – No Objection Certificate

Scope of Policy

This policy governs the usage of IT resources and services from an end user's perspective.

Objective

The objective of this policy is to ensure proper access and usage of IT resources and services by the end users.

1. Role and Responsibilities

Role to be performed by the IT Cell for implementing infrastructure and services:

1. To develop and implement different IT services across the University.
2. Administration of Internet services across the University.
3. Developing / procuring / administration of various required software for University automation process on regular basis.

Responsibilities need to be performed by the end user:

1. Responsible for carrying out functional aspect of the IT services.
2. The responsibility of maintenance and troubleshooting of desktop computers, all in one computers, laptop/notebook, printers, scanners and other related peripherals shall be carried out by the respective end user/department/unit.

2. Hardware Resources Policy

2.1 Introduction

The IT hardware resources include desktop computers, all in one computers, servers, laptop/notebook computers, thin client computers, wireless access points, Wireless adapters, network switch/hub, printers, scanners and other computer peripheral devices etc.



2.2 Scope of IT Hardware

The IT cell is responsible for buying and deploying the necessary IT hardware resources for providing IT services. The internet connectivity services shall be procured / deploy / carried out by IT Cell subject to the budgetary provisions.

Respective units and departments are responsible for procuring and maintaining hardware's like desktop computers, all in one computers, servers, laptop/notebook, printers, and scanners through appropriate university laid down purchase process.

Maintenance of network switch, rack, wireless routers, UTP cable, I/O box installed in respective units will be maintain by IT Cell. Cost of maintenance / replacement / extension will be executed by respective units through appropriate university laid down purchase process.

2.3 General Guidelines for end user

1. Computers shall normally be used only for executing University work. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.
2. Users shall ensure that updated licensed antivirus / scanning software is running in the systems.
3. Users shall abide by instructions or procedures as directed by the IT Cell from time to time.
4. End user cannot deploy / install network equipment in university network without prior permission of IT Cell.

2.4 Advisory Guide

1. Software installed on IT resources must be licensed software.

3. NAU IT Software Resources Policy and Guidelines

3.1 Introduction

This policy provides guidelines for the use of software for all employees/students within the NAU to ensure appropriate usage of it. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

3.2 General Guidelines

1. Users shall not copy or install any software on desktop devices including privately owned shareware and freeware without the approval of the IT Cell.
2. Users shall not share their accounts, passwords or similar information or devices which is used for identification and authorization purposes.



3. All software installation is to be carried out by end user only.
4. End Users should not use any VPN and Third party Software that exploit firewall and make NAU network vulnerable to the network attacks at NAU. If end user found out to carry out such malpractices than their account will be blocked / suspended on permanent basis.
5. End user is solely responsible for user level software Issues.

3.3 Advisory Guidelines

1. Users shall use strong password to defend against attacks.
2. Users shall not use pirated software.

4. Network Policy and Guidelines

4.1 Introduction

Navsari Agricultural University (NAU) Network is a wide area network that is comprised of buildings located at Navsari campus as well as that of remote stations using VPN technology. All the IT services delivered through this network medium from NAU server room. NAU network can be accessed through two modes wired network and wireless network. The policy for accessing wired and wireless network is as per given below.

4.2 Wired Network

Wired network comprises of fiber optic cable connectivity from server room to switch located at various buildings, from there the network is extended to switches or I/O box. The different roles and responsibilities for wired network are as per given below.

4.2.1 Responsibility of IT Cell

1. IT Cell is responsible to manage and administration of NAU wired network.
2. IT cell is responsible for Network connectivity up to department level.
3. The Network connectivity and the troubleshooting will be carried out by IT Cell subject to guidelines issued time by time.
4. Alteration / maintenance / extension activities in entire NAU network will be only carried out in the supervision of IT Cell.
5. IT Cell shall not responsible for failure in IT devices due to electricity issues at any place.

4.2.2 Responsibility of Unit / End User

1. The power supply to network equipment's and rack will be the sole responsibility of respective units.



2. Unit is not allowed to make changes in the network cabling at their premise without the consent of IT Cell and such activity will be treated as a network tempering.
3. No end user is allowed to share their internet service account with anyone.
4. Users shall not undertake any activity through any website or applications which is bypassing network security. Use of proxy server, VPN application or any other similar software will be counted as malpractices and in such case the account will be blocked / suspended on permanent basis.

4.3 Wireless Network

Any NAU Network service accessed through wireless device will be considered under this policy. The Wireless network services are the same as the wired network medium but accessed through wireless access point. The Wireless accessed device includes desktop computers with wifi connectivity, all in one computers, laptop/notebook computers, mobile tablets and mobile phones etc. For the wireless network access following responsibilities is given below.

4.3.1 Responsibility of IT Cell

1. The IT cell is responsible for Network connectivity up to department level.
2. The Network connectivity and the troubleshooting will be carried out by IT Cell subject to guidelines issued time by time.
3. Alteration / maintenance / extension activities in entire NAU network will be only carried out in the supervision of IT Cell.
4. IT Cell is not responsible for failure in IT devices due to electricity issues at any place.

4.3.2 Responsibility of Unit / end User

1. Department is responsible for providing power supply for the Wi-Fi Access Point.
2. The IT cell is not responsible for individual connectivity of end user's devices.
3. No end user is allowed to share their internet service account with anyone.
4. Users shall not undertake any activity through any website or applications which is bypassing network security. Use of proxy server, VPN application or any other similar software will be counted as malpractices and in such case the account will be blocked / suspended on permanent basis.

5. NAU IT Services and its Guidelines

Introduction

- The NAU is offering different kinds of services to employees. The services are developed, procured, deployed, administrated and managed by the IT cell.



5.1. NAU Web Mail

NAU is offering webmail services for NAU regular staff with domain "**nau.in**". The regular staff needs to register for the same service. Presently "**nau.in**" webmail service is hosted on Google server.

5.1.1 Role & Responsibilities of IT Cell

1. IT cell will administrate and maintain the NAU web mail services.
2. Regular staff looking to avail the "**nau.in**" webmail service shall send information to IT Cell through Head of the Unit as per issued guideline.
3. Any query regarding "**nau.in**" e-mail account shall be contacted to itcell@nau.in through head of the Unit (office) email.
4. In case a compromise of an e-mail ID is needed, the IT Cell reserves the right to reset the password of that particular e-mail ID if request comes from Unit Head login.
5. In case of a situation, when a compromise of an email ID impacts a large user base or the data security of the deployment, the IT Cell shall reset the password of that email ID. This action shall be taken on an immediate basis, and the information shall be provided to the user and the unit head subsequently.

5.1.2 General Guidelines

1. All users accessing the e-mail services must use strong passwords for security of their e-mail accounts.
2. Users shall ensure that e-mails are kept confidential. Users must ensure that information regarding their password or any other personal information is not shared with anyone.
3. Auto-save of password in the Organization e-mail service shall not be permitted due to security reasons.

5.1.3 NAU Web Mail Guidelines

1. User's shall not exchange e-mails that might be categorized as harassing, obscene or threatening must be avoided.
2. Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information will be considered inappropriate.
3. Unauthorized access of the services will be considered inappropriate. This includes the distribution of e-mails anonymously, use of other officers' user IDs or using a false identity.



4. Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail will be considered inappropriate.
5. Creation and exchange of information in violation of any laws, including copyright laws will be considered inappropriate.
6. Willful transmission of an e-mail containing a computer virus will be considered inappropriate and must be avoided.
7. Misrepresentation of the identity of the sender of an e-mail will be considered inappropriate and must be avoided.
8. Use or attempt to use the accounts of others without their permission will be considered inappropriate and must be avoided.
9. 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 will be considered inappropriate and must be avoided.
10. Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation of the account.
11. The User is responsible for any data/e-mail that is transmitted using the Organization e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.
12. Users should not share passwords.
13. In case of threat to the security, the e-mail id being used to impact the service may be suspended or deactivated immediately by the IT Cell.
14. Subsequent to deactivation, the concerned user and the Unit Head will be informed.
15. In case of retirement / death / resignation of staff from the University, Unit Head has to send the details of concerned to the IT Cell for deactivation of respective staff member email ID.

5.2. Online Examination Software

This Online examination software is a service which is technically managed by the IT Cell and functionally administered by the Registrar Office. The IT Cell is only responsible for technical support of the service.



5.2.1 General Guidelines

1. The responsibility of the functional aspects of the Online Examination software shall be looked after by Registrar Office, Navsari Agricultural University.
2. The Technical aspects shall be the sole responsibility of IT Cell.
3. Users of this service is bound by the periodically guidelines issued by the Registrar Office and the IT Cell for using the service.
4. The decision of the Registrar Office should be final in using this service.

5.3. Online Tour Management Software

Online Tour Management software is a service helpful for the online application of tour as per the NAU statutory guidelines. The IT Cell is only responsible for technical support to users.

General Guidelines

1. The IT Cell shall carry out technical support and troubleshooting of the service.
2. Respective unit head is responsible for management of user accounts of his / her unit.
3. The users shall follow the guidelines and instructions issued by IT Cell at regular interval for the use of the service.

5.4 Online ERP service

Online ERP service deployed at NAU deals with the entire online financial services pay bill, Online GPF, Pension, Financial Accounting, Expenditure, Income and Grant services, etc.

General Guidelines

1. IT cell is responsible to carry out technical aspects of the online ERP systems.
2. Comptroller office and respective users of different units are responsible for financial aspects of the online ERP systems.
3. Registrar office and respective users of different units are responsible for administrative aspects of the online ERP systems.
4. The Users should abide by the different guidelines issued from time to time by concerned office.

6. NAU Network Monitoring and privacy Policy

The purpose of network monitoring is to identify and block malicious activity in order to protect the NAU network. In order to protect data, IT Cell may use network monitoring technologies (Firewall) to log network activity and to scan data moving across the network. These technologies may include anti-virus software, firewalls, intrusion protection and intrusion detection systems, vulnerability management systems, and database and application monitoring systems. This information may be used for identifying inappropriate use of Internet services through network. Confidentiality of all information gathered as a result of network monitoring will be maintained at all times. Access to information obtained through network monitoring will



be limited to IT Cell and in the event of an investigation, shared with the due permission of Head of the University.

6.1 Network Monitoring Guidelines

1. IT Cell shall monitor user's online activities on NAU network to prevent the misuse of Internet service.
2. If end user is surfing unwanted content (pornography, movie, music, songs, games, sexist, or other such type media) then their internet account will be suspended.

6.2 Social Networking Monitoring Policy

1. Use of social networking sites by Organization is governed by "Framework and Guidelines for use of Social Media for Government Organizations" available at <http://deity.gov.in>.
2. User shall comply with all the applicable provisions under the IT Act 2000, while posting any data pertaining to the Organization on social networking sites.
3. User shall not post any material that is offensive, threatening, and obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
4. User shall not disclose or use any confidential information obtained in their capacity as an employee/user of the Organization.
5. Social networking websites and highly bandwidth consuming websites are strictly prohibited during office hours.

7. IT Security Policy

A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and data. IT cell reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system.

Scrutiny/Release of logs

IT Cell shall neither accept nor act on the request from any other Organization without prior permission from competent authority for scrutiny or release of logs.

8. Internet Services

8.1 Internet Registration Service

1. NAU staff members have to register for internet service account through tour management software only. Once staff has applied for registration, IT Cell will approve the same and send login id and password to the concerned staff's mobile number.
2. NAU students have to register for internet service account through NAU website only, in which they have to enter the details of enrollment number and mobile number. Once student has applied for registration, IT Cell will approve the same if student enrollment number and mobile number matches with the academic registration data and will send login id and password to the concerned student's mobile number.



8.2 NOC (Closure of Internet Service)

1. In case of retirement / death / resignation of staff from the University, Unit head has to send the details of concerned to the IT Cell for deactivation of respective staff member's login.
2. It is compulsory to take NOC (stop internet service) for every students before submission of thesis or completion of final examination and that too shall be taken care by respective Guide / Principal of students.
3. Those students having internet registration account have to apply for NOC through NAU website, once it is applied, IT Cell will approve the same if no misuse is done through students internet account.
4. Student which has not applied for internet registration can take NOC from IT Cell through their respective Guide or Principal.

9. Enforcement and Deactivation Policy

Enforcement

This policy is applicable to all users of Organization. It is mandatory for all users to adhere to the provisions of this policy. Organization shall be responsible for ensuring compliance with the provisions of this policy. The IT Cell shall provide necessary technical assistance to the Organizations in this regard.

Deactivation

In case of any threat to security of the Organization's systems or network from the resources and services being used by a user, the resources and services being used may be deactivated immediately by the IT cell. Subsequent to such deactivation, the concerned user and the competent authority of Organization shall be informed.

10. E-Waste

Electronic waste include desktop computer, laptop, printer, UPS, batteries, scanner, network equipment's, servers, firewall, projector, IT and Audio / Visual aid related items, etc.

General Guidelines

1. Unit / department heads are responsible to carry out e-waste as per the guidelines published by the government.
2. Unit / department heads are responsible to carry out necessary procedure for disposal of e-waste.