Gujarat Biotechnology University
An initiative of Department of Science and Technology,
Government of Gujarat

No: GBU/ADM/IT/188/2023-24/827 **Date: 26/11/2024**

Circular

Subject: Cyber Security Guidelines to Secure IT Assets

Reference: Circular No: DST/ADV/e-file/24/2024/0599/E-Governance, dated: 20/11/2024

In reference to the above-mentioned circular issued by the Department of Science & Technology (DST), it is proposed to issue a comprehensive cybersecurity guideline.

The guidelines are imperative in the current digital landscape, where rapid advancements in technology—such as digital transformation, cloud computing, artificial intelligence (AI), and remote work—have both simplified operations and increased vulnerabilities to cyber threats.

Key Highlights of the Cybersecurity Guidelines:

1. **Desktop/Laptop and Printer Security at Office:** Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work**.** Desktop must be locked/logged off when the workspace is unoccupied and must be shut down if not in use. Printer to be configured to disallow storing of print history.
2. **Antivirus Usage**: Emphasizing the importance of updated antivirus software.
3. **Password Management**: Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
4. **Cybersecurity Resources**: Providing tools and resources for enhanced security etc.

These guidelines are designed to safeguard IT systems, networks, and data while promoting cybersecurity awareness among all employees and faculty. This measure ensures alignment with the directive received from DST and bolsters the cybersecurity framework at GBU. All employees are required to adhere to this guideline.

This circular has been approved by the Hon. Director General vide approved note GBU/ITS/e-file/265/2024/0384/Admin/note21 dated 25/11/2024.

-Sd/-
Registrar

Attachment: DST Circular for cyber-Security guidelines dated 20/11/2024

To,
1. **All GBU Faculties**
2. **All GBU Staff (including contractual and outsourced staff)**

Phone: +91 99099 57407 (General Query)
Email: info-gbu@gujarat.gov.in
Website: www.gbu.edu.in

Gujarat International Finance Tec-City (GIFT city),
Gandhinagar, Gujarat -382355, INDIA

રાજ્ય સરકારના આઇ.ટી. એસેટ્સને સુરક્ષિત કરવા અંગેની સાયબર સુરક્ષા માર્ગદર્શિકા(Cyber Security Guideline) બહાર પાડવા બાબત.

ગુજરાત સરકાર

વિજ્ઞાન અને પ્રદ્યોગિકી વિભાગ

ઠરાવ ક્રમાંક: DST/ADV/e-file/24/2024/0599/E-Governance

સચિવાલય ગાંધીનગર

તા.૨૦.૧૧.૨૦૨૪

વંચાણે લીધો:

(૧) નિયામક આઇ.સી.ટી. અને ઇ-ગવર્નન્સની કચેરીનો તા.૧૨.૦૭.૨૦૨૪ નો પત્ર ક્રમાંક: ICT/0010/06/2024

પરિપત્ર:-

ડિજિટલ યુગમાં ટેક્નોલોજીનો વિકાસ ડિજિટલ ટ્રાન્સફોર્મેશન, ક્લાઉડ કમ્પ્યુટિંગ, આર્ટિફિશિયલ ઇન્ટેલીજન્સ(AI) અને રિમોટ વર્ક જેવા વિવિધ રૂપોમાં થઈ રહ્યો છે. ટેક્નોલોજી દ્વારા જીવન અને વ્યવસાય વધુ સરળ બન્યા છે, જો કે આ સાથે જ સાયબર થ્રેટ્સનો વિશ્વભરમાં નોંધપાત્ર વધારો થયો છે. આઇ.ટી. નેટવર્ક, સિસ્ટમ્સ અને ડેટાને અસર કરતા સાયબર થ્રેટ્સનું વધતું જોખમ ઇ-ગવર્નન્સને નુકશાનકારક બની શકે છે. આથી, ગુજરાત સરકારના "ઇ-ગવર્નન્સ, ગુડ ગવર્નન્સ"ના સપનાને સાકાર કરવા તમામ વિભાગો/વિભાગ હસ્તકની કચેરીઓ/બોર્ડ/જાહેર સાહસો/નિયંત્રણ હેઠળની સંસ્થાઓના તમામ અધિકારી/કર્મચારીઓને(આઉટસોર્સિંગ/ કરાર આધારિત નિમણૂક પામેલ કર્મચારી સહિત) સાયબર સુરક્ષા માર્ગદર્શન મળી રહે તે હેતુસર સાયબર સુરક્ષા માર્ગદર્શિકા અંગ્રેજી તથા ગુજરાતીમાં આથી બહાર પાડવામાં આવે છે.

૨. આ માર્ગદર્શિકાનો ઉદ્દેશ્ય સુરક્ષિત ઇન્ફોર્મેશન એન્ડ કોમ્યુનિકેશન ટેક્નોલોજી(ICT) ઇકોસિસ્ટમ બનાવવાનો છે. જે રાજ્યના આઇ.ટી. ઇન્ફ્રાસ્ટ્રક્ચરને મજબૂત બનાવવા માટે જરૂરી પગલાંઓ દર્શાવે છે તથા સાયબર થ્રેટ્સ સામે રક્ષણ પ્રદાન કરશે અને ઇ-ગવર્નન્સને વધુ સુરક્ષા પૂરી પાડશે.

૩. તમામ વિભાગ હેઠળની કચેરીઓએ સાયબર સુરક્ષા માર્ગદર્શિકાનું ચુસ્તપણે પાલન કરવાનુ રહેશે તથા તેને સુનિશ્ચિત કરવાની જવાબદારી જે-તે વિભાગ/ખાતા/કચેરીના વડાની રહેશે.

ગુજરાતના રાજ્યપાલશ્રીના હુકમથી અને તેમના નામે,

(એન.એચ.ગઢવી)
સંયુક્ત સચિવ
વિજ્ઞાન અને પ્રૌદ્યોગિકી વિભાગ
ગુજરાત સરકાર

બિડાણ: ઉપર મુજબ

પ્રતિ,

૧.માન. રાજ્યપાલશ્રીના અગ્રસચિવશ્રી, રાજભવન, ગાંધીનગર.

૨.માન. મુખ્યમંત્રીશ્રીના અધિક મુખ્ય સચિવશ્રી, સ્વર્ણિમ સંકુલ –૧, સચિવાલય, ગાંધીનગર.

૩.મુખ્ય સચિવશ્રીના અધિક સચિવશ્રી, સચિવાલય, ગાંધીનગર.

૪.અધિક મુખ્ય સચિવશ્રી/અગ્ર સચિવશ્રી/સચિવશ્રી, સર્વે વહીવટી વિભાગો, સચિવાલય, ગાંધીનગર.(સચિવાલયના તમામ વિભાગોની તમામ શાખાઓ તથા વિભાગ હસ્તકના તમામ કચેરીઓ/બોર્ડ/કોર્પોરેશન/ સોસાયટીના સંબંધિત અધિકારીઓ/ કર્મચારીઓના ધ્યાને મુકવા સારુ)

૫.સેક્શન અધિકારીશ્રી, સંકલન શાખા, વિજ્ઞાન અને પ્રૌધોગિકી વિભાગ, સચિવાલય, ગાંધીનગર. (વિભાગ હસ્તકના તમામ કચેરીઓ/બોર્ડ/કોર્પોરેશન/ સોસાયટીના સંબંધિત અધિકારીઓ/ કર્મચારીઓના ધ્યાને મુકવા સારુ)

૬. શાખા સિલેક્ટ ફાઈલ.

सत्यमेव जयते
ગુજરાત સરકાર
Government of Gujarat

રાજયના આઇટી અસ્ક્યામતો (એસેટ્સ)ને સુરક્ષિત કરવા અંગેની સાયબર સુરક્ષા માર્ગદર્શિકા

વિજ્ઞાન અને પ્રૌદ્યોગિકી વિભાગ

(પરિપત્ર ક્રમાંક: DST/ADV/e-file/24/2024/0599/E-Governance, તા.૨૦/૧૧/૨૦૨૪)

વિજ્ઞાન અને પ્રોદ્યોગિકી વિભાગ
ગુજરાત સરકાર
વર્ષ: ૨૦૨૪
બ્લોક નં –૭/૫, સરદાર પટેલ ભવન, સચિવાલય, ગાંધીનગર
Website: https://dst.gujarat.gov.in/

અનુક્રમણિકા

- **સંક્ષિપ્ત શબ્દો**

GoG/state	Government of Gujarat
DST	Department of Science & Technology, GoG
GoI	Government of India
Meity	Ministry of Electronics & IT, GoI
GSWAN	Gujarat State Wide Area Network
GSDC	Gujarat State Data centre
OS	Operating System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secured
BIOS	Basic Input Output System
VPN	Virtual Private Network
USB	Universal Serial Bus
ICT	Information and Communication Technology
CERT	Computer Emergency Response Team
HoD	Head of Department
URL	Uniform Resource Locator
OEM	Original Equipment Manufacturer
UIDAI	Unique Identification Authority of India, GoI
GPS	Global Positioning System
NFC	Near Field Communication
AI	Artificial Intelligence
CISO	Chief Information Security Officer
DIT	Directorate of ICT & e-Governance
GSOC	Gujarat Security Operation Center

- **પ્રસ્તાવના**

ડિજિટલ યુગમાં ટેક્નોલોજીનો વિકાસ – ડિજિટલ ટ્રાન્સફોર્મેશન, ક્લાઉડ કમ્પ્યુટિંગ, આર્ટિફિશીયલ ઇન્ટેલિજન્સ (AI) અને રિમોટ વર્ક જેવા વિવિધ રૂપોમાં થઈ રહ્યો છે. ટેક્નોલોજી દ્વારા જીવન અને વ્યવસાય વધુ સરળ બન્યા છે, જો કે આ સાથે જ સાયબર થ્રેટ્સનો વિશ્વભરમાં નોંધપાત્ર વધારો થયો છે. આઇટી નેટવર્ક, સિસ્ટમ્સ અને ડેટાને અસર કરતા સાયબર થ્રેટ્સનું વધતું જોખમ ઇ–ગવર્નન્સને નુકશાનકારક બની શકે છે.

આ માર્ગદર્શિકા રાજ્યમાં સાયબર સુરક્ષિત ઈન્ફોર્મેશન એન્ડ કોમ્યુનિકેશન ટેક્નોલોજી(ICT) ઈકોસિસ્ટમ બનાવવાના ઉદ્દેશ્ય સાથે તૈયાર કરવામાં આવી છે. આ માર્ગદર્શિકા રાજ્યના આઇટી ઈન્ફ્રાસ્ટ્રક્ચરને મજબૂત બનાવવા માટે જરૂરી પગલાંઓ દર્શાવે છે, જે સાયબર થ્રેટ્સ સામે રક્ષણ પ્રદાન કરશે અને ઇ–ગવર્નન્સને વધુ સુરક્ષા પૂરી પાડશે.

1.કાર્યક્ષેત્ર

આ માર્ગદર્શિકાનું ગુજરાત સરકાર (GoG)ના તમામ વિભાગો/ ખાતાના વડાની કચેરીઓ/ બોર્ડ/ જાહેર સાહસો (PSU)/ નિયંત્રણ હેઠળની સંસ્થાઓના તમામ અધિકારીઓ/કર્મચારીઓએ (આઉટસોર્સિંગ/કરારના ધોરણે નીમાયેલા કર્મચારીઓ સહિત) પાલન કરવાનું રહેશે.

2. ઓફિસમાં ખાતે ડેસ્કટોપ/લેપટોપ અને પ્રિન્ટરની સિક્યોરિટી

2.1 નિયમિત કામ માટે કમ્પ્યુટર/લેપટોપ એક્સેસ કરવા માટે માત્ર non-admin એકાઉન્ટનો ઉપયોગ કરવો. જરુર જણાયે યોગ્ય સત્તાધિકારીની મંજૂરી સાથે વપરાશકર્તાઓને એડમિન ઍક્સેસ આપવો.

2.2 કમ્પ્યુટર સિસ્ટમ બુટ કરવા માટે BIOS પાસવર્ડ સેટ કરવો.

2.3 ઓપરેટિંગ સિસ્ટમ અને BIOS ફર્મવેર નવીનતમ અપડેટ્સ/પેચ સાથે અપડેટ થયેલ છે કે કેમ તેની ખાતરી કરવી.

2.4 તમામ સરકારી કચેરીઓમાં GSWAN નેટવર્ક સાથે જોડાયેલ સિસ્ટમ્સ પર URL http://gswan.gujarat.gov.in/ પરથી DST દ્વારા ઉપલબ્ધ કરવામાં આવેલ એન્ટિવાયરસ ક્લાયન્ટ/સોફ્ટવેર ઇન્સ્ટોલ કરવું અને તેને લેટેસ્ટ વાયરસ ડેફિનેશન, સિગ્નેચર અને patch સાથે અપડેટ રાખવું.

2.5 આપના કચેરી સાથે સંકળાયેલ કાર્ય માટે જરૂરી એપ્લિકેશન્સ/સોફ્ટવેર જ ઇન્સ્ટોલ કરવા તથા અન્ય કોઈપણ એપ્લિકેશન/સોફ્ટવેર ઇન્સ્ટોલ કરવા નહીં.

2.6 જ્યારે વર્કસ્પેસ ખાલી હોય ત્યારે ડેસ્કટૉપ જરુરી લૉક/લૉગ ઑફ કરવુ અને જો ઉપયોગમાં ન હોય તો તેને બંધ કરવું.

2.7 ડેસ્કટોપ/લેપટોપ અને પ્રિન્ટરના સોફ્ટવેરને નવીનતમ અપડેટ્સ/પેચ સાથે અપડેટ રાખવા.

2.8 તમામ પ્રિન્ટરો અને ફેક્સ મશીન પરથી પ્રિન્ટ થતાંની સાથે જ પ્રિન્ટર ટ્રે/ ફેક્સ ટ્રે પરના કાગળો દૂર કરવા. પ્રતિબંધિત અથવા સંવેદનશીલ માહિતી ધરાવતા પ્રિન્ટઆઉટ પ્રિન્ટ થતાંની સાથે જ પ્રિન્ટરમાંથી દૂર કરવા જોઈએ.

2.9 Shared પ્રિન્ટર માટે યુનિક પાસ કોડ સેટ કરવો.

2.10 નેટવર્ક પ્રિન્ટરનું ઈન્ટરનેટ સાથે જોડાણ સિકયોર કરવું.

2.11 પ્રિન્ટર કન્ફીગરેશનમાં હિસ્ટ્રી સ્ટોરેજ રાખવું નહીં.

2.12 ઇન્ફોર્મેશન ઍક્સેસને નિયંત્રિત કરવા માટે ડેસ્કટોપ ફાયરવોલ એનેબલ કરવું.

2.13 ડેસ્કટોપ/લેપટોપ અને મોબાઈલ ફોન પર GPS, બ્લૂટૂથ, NFC અને અન્ય સેન્સર્સને ડિસેબલ રાખવા તેમજ જરૂરી જણાયે જ તેનો ઉપયોગ કરવો.

2.14 સ્ટેટ ડેટા સેન્ટરમાં સ્થિત કોઈપણ IT એસેટ સાથે કનેક્ટ કરવા માટે GSDC દ્વારા પૂરી પાડવામાં આવેલ VPN સેવાનો ઉપયોગ કરવો અને VPN સેવા માટે ઉપયોગમાં લેવાનાર સિસ્ટમ અદ્યતન એન્ટિવાયરસ સૉફ્ટવેરથી અપડેટ રાખવી.

2.15 આંતરિક સરકારી દસ્તાવેજોને સ્કેન કરવા માટે કોઈપણ બાહ્ય મોબાઈલ એપ્લિકેશન આધારિત સ્કેનર સેવાઓ (ઉદા: કેમ સ્કેનર) નો ઉપયોગ કરવો નહીં.

2.16 પાઈરેટેડ ઓપરેટિંગ સિસ્ટમ્સ અને સોફ્ટવેર/એપ્લિકેશનનો ઉપયોગ કરવો નહીં.

2.17 કોઈપણ અસુરક્ષિત સામગ્રી પર કોઈપણ પાસવર્ડ્સ, IP એડ્રેસ, નેટવર્ક ડાયાગ્રામ અથવા અન્ય સંવેદનશીલ માહિતી લખવી નહીં (દા.ત: સ્ટીકી/પોસ્ટ-ઇટ નોટ્સ, સાદા કાગળ અથવા પિન કરેલા અથવા તમારા ટેબલ પર પોસ્ટ કરેલા કાગળ) અને તેને કોઈપણ અનધિકૃત વ્યક્તિ સાથે શેર કરવી નહીં.

2.18 મહત્વપૂર્ણ ડેટાનો નિયમિત ઓફલાઇન બેકઅપ લેવો.

3.પાસવર્ડ મેનેજમેન્ટ

3.1 કેપિટલ અક્ષરો, નાના અક્ષરો, સંખ્યાઓ અને વિશિષ્ટ અક્ષરોના સંયોજનનો ઉપયોગ કરીને ઓછામાં ઓછા 8 અક્ષરો ધરાવતા જટિલ પાસવર્ડ્નો ઉપયોગ કરવો.

3.2 જ્યાં ઉપલબ્ધ હોય ત્યાં મલ્ટી–ફેક્ટર ઓથેન્ટિકેશનનો ઉપયોગ કરવો.

3.3 વપરાશકર્તાઓએ તેમના દરેક કાર્ય સંબંધિત એકાઉન્ટ માટે અલગ, યુનિક પાસવર્ડનો ઉપયોગ કરવો આવશ્યક છે.

3.4 ઇન્ટરનેટ બ્રાઉઝરમાં અથવા કોઈપણ અસુરક્ષિત દસ્તાવેજોમાં પાસવર્ડ, પેમેન્ટ, ક્રેડિટ/ડેબિટ કાર્ડ સંબંધિત માહિતી અથવા કોઈપણ મહત્વપૂર્ણ ડેટા સેવ કરવો નહીં.

3.5 પાસવર્ડ ગુપ્ત રાખવો અને શેર કરવો નહીં.

4.ઇન્ટરનેટ બ્રાઉઝિંગ સિક્યોરિટી

4.1 સરકારી એપ્લિકેશન્સ/સેવાઓ, ઈમેલ સેવાઓ, બેંકિંગ/ચુકવણી સંબંધિત સેવાઓ અથવા અન્ય કોઈપણ મહત્વપૂર્ણ એપ્લિકેશન/સેવાઓ ઍક્સેસ કરતી વખતે, બ્રાઉઝરમાં પ્રાઈવેટ બ્રાઉઝિંગ/ઈનકોગ્નિટો (incognito) મોડનો ઉપયોગ કરવો હિતાવહ છે.

4.2 યુઝર લોગીન જરૂરી હોય તેવી સાઇટ્સને એક્સેસ કરતી વખતે, કોઈપણ લિંક પર ક્લિક કરવાને બદલે હંમેશા બ્રાઉઝરના એડ્રેસ બાર પર મેન્યુઅલી સાઇટનું ડોમેઈન નામ/URL ટાઇપ કરવુ.

4.3 ઇન્ટરનેટ બ્રાઉઝરના લેટેસ્ટ વર્ઝનનો ઉપયોગ કરવો અને ખાતરી કરવી કે બ્રાઉઝર લેટેસ્ટ અપડેટ્સ/પેચ સાથે અપડેટ થયેલ છે.

4.4 કોઈપણ થર્ડ પાર્ટી અજ્ઞાત સેવાઓનો ઉપયોગ કરવો નહીં (ઉદા.: Nord VPN, Express VPN, Tor, Proxies વગેરે).

4.5 ઇન્ટરનેટ બ્રાઉઝરમાં કોઈપણ થર્ડ પાર્ટી ટૂલબાર અને એક્સ્ટેંશન/પ્લગઈન્સ (ઉ.દા.: ડાઉનલોડ મેનેજર, વેધર ટૂલ બાર વગેરે)નો ઉપયોગ કરવો નહીં.

4.6 ઇન્ટરનેટ પરથી કોઈપણ અનઅધિકૃત અથવા પાઇરેટેડ સામગ્રી/સોફ્ટવેર ડાઉનલોડ કરવી નહીં. (ઉદા: પાઇરેટેડ મૂવીઝ, ગીતો, ઇ–બુક્સ, સોફ્ટવેર)

4.7 કોઈપણ ગેમ ઇન્સ્ટોલ કરવા અથવા રમવા માટે સિસ્ટમનો ઉપયોગ કરવો નહીં.

4.8 કોઈપણ સંક્ષિપ્ત કરેલ URL (ઉદા: tinyurl.com/ab534/) અથવા પોપઅપ વિન્ડો ખોલતી વખતે સાવચેતી રાખવી. ઘણા માલવેર અને ફિશિંગ સાઇટ્સ URL શોર્ટનર સેવાઓનો દુરુપયોગ કરે છે. આવી લિંક્સ ફિશિંગ/માલવેર વેબપેજ તરફ દોરી શકે છે, જે તમારા ઉપકરણ ને નુકસાન પહોંચાડી શકે છે.

5.મોબાઇલ સિક્યોરિટી

5.1 મોબાઇલ ઓપરેટિંગ સિસ્ટમ ફક્ત વિશ્વસનીય સ્ત્રોતોમાંથી જ લેટેસ્ટ ઉપલબ્ધ અપડેટ્સ/પેચ સાથે અપડેટ થયેલ હોય તેની ખાતરી કરવી.

5.2 મોબાઇલ ફોન પર Wi-Fi, GPS, Bluetooth, NFC અને અન્ય સેન્સર્સને ડીસેબલ રાખવા. જ્યારે જરૂરીયાત હોય ત્યારે જ એનેબલ કરવા.

5.3 Google (Android માટે) અને Apple (iOS માટે) ના અધિકૃત એપ સ્ટોરમાંથીજ એપ્સ ડાઉનલોડ કરવી.

5.4 બ્લૂટૂથ પેરિંગ અથવા ફાઇલ શેરિંગ માટે કોઈપણ અજાણી રીકવેસ્ટ સ્વીકારવી નહીં.

5.5 એપ ઇન્સ્ટોલ કરતા પહેલા, એપ દ્વારા જરૂરી ડીવાઈઝ પરમીશનને કાળજીપૂર્વક વાંચવી અને સમજવી.

5.6 રીકવેસ્ટ કરેલ પરમીશન્સ અને એપ દ્વારા પૂરી પાડવામાં આવેલ ફંકશનાલીટી વચ્ચે કોઈ અસમાનતાના કિસ્સામાં, એપ ઇન્સ્ટોલ ન કરવી અથવા જરૂરી પરમીશન આપવી અથવા ફક્ત એપનો ઉપયોગ કરતી વખતે જ પરમીશન આપવી. (ઉદા.: કેલ્ક્યુલેટર એપ્લિકેશનમાં GPS & Bluetooth ઉપયોગ થતો ન હોઈ તે પ્રકારની પરમીશન આપવી નહી).

5.7 મોબાઇલ ઉપકરણનો યુનિક ૧૫–અંકનો IMEI નંબર નોંધો અને તેને ઑફલાઇન રાખો. તે મોબાઇલ ઉપકરણના ફિઝીકલ નુકસાન અને ચોરીના કિસ્સામાં જાણ કરવા માટે ઉપયોગી થઈ શકે છે.

5.8 મોબાઇલ ફોનના ઍક્સેસને પ્રતિબંધિત કરવા માટે પાસ કોડ/સિક્યોરિટી પેટર્ન/બાયોમેટ્રિક્સ દ્વારા ફોન અથવા કીપેડ માટે ઑટો લૉકનો ઉપયોગ કરવો.

5.9 મોબાઇલ ટ્રેકિંગની સુવિધાનો ઉપયોગ કરો જે તમારી પસંદગીના બે પહેલાથી પસંદ કરેલા ફોન નંબર પર આપમેળે મેસેજ મોકલે છે, જે મોબાઇલ ફોન ખોવાઈ જાય/ચોરી થઈ જાય તો મદદ કરી શકે છે. વૈકલ્પિક રીતે Find My Device ફંક્શનાલીટી(જો ઉપલબ્ધ હોય તો)નો ઉપયોગ કરી શકો છો.

5.10 ફોનનો નિયમિત ઓફલાઇન બેકઅપ લેવો.

5.11 કોમ્પ્યુટરમાંથી મોબાઈલમાં ડેટા ટ્રાન્સફર કરતા પહેલા, ડેટાને લેટેસ્ટ અપડેટ્સ ધરાવતા એન્ટિવાયરસથી સ્કેન કરવો.

5.12 SMS, QR કોડ્સ અથવા સોશિયલ મીડિયા વગેરે દ્વારા શેર કરવામાં આવેલી કોઈપણ લિંકને ખોલતી વખતે સાવધાની રાખો, આ પ્રકારની લિંક્સ પહેલા આકર્ષક ઑફર્સ/ડિસ્કાઉન્ટ વગેરે હોય, અથવા કોઈપણ લેટેસ્ટ સમાચાર વિશે વિગતો પ્રદાન કરે છે. આવી લિંક્સ ફિશિંગ/માલવેર વેબપેજ તરફ દોરી શકે છે, જે તમારા ઉપકરણને કોમ્પ્રોમાઈઝ કરી શકે છે.

5.13 ખોવાયેલા અથવા ચોરાયેલા ઉપકરણોની તાત્કાલિક નજીકના પોલીસ સ્ટેશન અને સંબંધિત સર્વિસ પ્રોવાઇડરને જાણ કરવી.

5.14 તમારા ફોનમાં ઓટોમેટિક ડાઉનલોડ્સને ડીસેબલ રાખવું.

5.15 મોબાઇલ સોફ્ટવેરને હંમેશા અધિકૃત OEM તરફથી અપડેટ રાખવા.

6. ઈ–મેઇલ સિક્યોરિટી

6.1 કોઈપણ વ્યક્તિ સાથે ઈ–મેઇલ પાસવર્ડ શેર કરવો નહીં.

6.2 સત્તાવાર વાર્તાલાપ માટે કોઈપણ અનઅધિકૃત/બાહ્ય ઈ–મેઇલ સેવાઓનો ઉપયોગ કરવો નહીં.

6.3 અજાણ્યા સેન્ડર દ્વારા મોકલવામાં આવેલ ઈ–મેઇલમાં સમાવિષ્ટ કોઈપણ લિંક અથવા એટેચમેન્ટને ક્લિક કરવા/ખોલવા નહીં.

6.4 અજાણ્યા, શંકાસ્પદ અથવા અવિશ્વસનીય સ્ત્રોતમાંથી ઈ–મેઇલ સાથે જોડાયેલ કોઈપણ ફાઇલ અથવા મેક્રો ક્યારેય ખોલવા નહીં. અટેચમેન્ટ તરીકે ડાઉનલોડ કરતી વખતે અથવા બિનવિશ્વસનીય સ્ત્રોતમાંથી પ્રાપ્ત થતાં મેક્રો ધરાવતા ડૉક્યુમેન્ટ સાથે સાવધાની રાખવી, હંમેશા "મેક્રોને ડીસેબલ કરો" વિકલ્પ પસંદ કરવો અને MS Office જેવી તમારી ઓફિસ પ્રોડકટીવિટી એપ્લિકેશન પર સુરક્ષિત મોડ એનેબલ છે તેની ખાતરી કરવી.

6.5 થર્ડ પાર્ટી ઈ–મેઇલ સિસ્ટમ પર આપમેળે ઇમેઇલ ફોરવર્ડ કરવા ડીસેબલ વિકલ્પ રાખવો.

6.6 કોઈપણ વ્યક્તિગત ઉપયોગ માટે સરકાર દ્વારા આપવામાં આવેલ સત્તાવાર ઈ–મેઇલ આઈડીનો ઉપયોગ કરવો નહીં.

7. રીમુવેબલ મીડિયા સિક્યોરિટી

7.1 પ્રથમ વખત ઉપયોગ કરતા પહેલા રીમુવેબલ મીડિયા જેવા કે પોર્ટેબલ હાર્ડડિસ્ક, P.D., C.D. વગેરેને ફોર્મેટ કરવા.
7.2 રીમુવેબલ મીડિયાની સામગ્રીને કાઢી નાખવા માટે સુરક્ષિત વાઇપ કરવી.
7.3 રીમુવેબલ મીડિયા એક્સેસ કરતા પહેલા એન્ટીવાયરસ સોફ્ટવેર વડે સ્કેન કરવા.
7.4 હંમેશા તમારા ડૉક્યુમેન્ટને મજબૂત પાસવર્ડથી સુરક્ષિત કરવા.
7.5 કોઈપણ અનધિકૃત ઉપકરણો પર રીમુવેબલ મીડિયાને પ્લગ–ઇન કરવા નહીં.

8. સોશિયલ મીડિયા સિક્યોરિટી

8.1 સોશિયલ મીડિયા અને નેટવર્કિંગ સાઇટ્સ ઍક્સેસ કરતી વખતે વ્યક્તિગત માહિતીના ઉપયોગ/એક્સ્પોઝરને મર્યાદિત અને નિયંત્રિત કરવા.
8.2 મિત્ર/સંપર્ક તરીકે રીકવેસ્ટ સ્વીકારતા પહેલા હંમેશા વ્યક્તિની અધિકૃતતા તપાસવી.
8.3 સોશિયલ મીડિયા એકાઉન્ટ્સને સુરક્ષિત કરવા માટે મલ્ટી–ફેક્ટર ઓથેન્ટિકેશનનો ઉપયોગ કરવો.
8.4 કોઈપણ અજાણ્યા સંપર્ક/વપરાશકર્તા દ્વારા મોકલવામાં આવેલી લિંક્સ અથવા ફાઇલો પર ક્લિક કરવી/ ખોલવી નહી.
8.5 કોઈપણ આંતરિક સરકારી દસ્તાવેજો અથવા સોશિયલ મીડિયા પર જાહેર જનતા માટે ન હોય તેવી કોઈપણ માહિતી પ્રકાશિત અથવા પોસ્ટ કરવી નહીં અથવા શેર કરવી નહીં.
8.6 સોશિયલ મીડિયા દ્વારા કોઈપણ વણચકાસાયેલ માહિતી પ્રકાશિત અથવા પોસ્ટ કરવી નહીં અથવા શેર કરવી નહીં.
8.7 કોઈપણ સોશિયલ મીડિયા પ્લેટફોર્મ પર સત્તાવાર(official) ઈમેલ એડ્રેસ શેર કરવો નહીં.
8.8 વિજ્ઞાન અને પ્રોદ્યોગિકી વિભાગ દ્વારા વખતોવખત બહાર પાડવામાં આવતી સૂચના/માર્ગદર્શિકાઓનું પાલન કરવું.

9. એન્ટિવાયરસ વપરાશ

9.1 વપરાશકર્તાએ વિજ્ઞાન અને પ્રોદ્યોગિકી વિભાગનું એન્ટરપ્રાઇઝ ગ્રેડ એન્ડપોઇન્ટ એન્ટીવાયરસ સોલ્યુશન ઇન્સ્ટોલ કરવું.

9.2 વપરાશકર્તા દ્વારા https://gswan.gujarat.gov.in/ પરથી એન્ટિવાયરસ સોલ્યુશન ડાઉનલોડ કરી શકાશે.

9.3 વપરાશકર્તાએ ઉપરોક્ત એન્ટિવાયરસનો ઉપયોગ કરીને તેના કમ્પ્યુટરને સમયાંતરે સંપૂર્ણ સ્કેન કરવું.

9.4 વપરાશકર્તાએ ઉપરોક્ત એન્ટિવાયરસ સોલ્યુશન સિવાય તેમની સિસ્ટમ પર ઇન્સ્ટોલ કરેલ કોઈપણ અન્ય એન્ટિવાયરસ સોફ્ટવેરને અનઇન્સ્ટોલ કરવું.

9.5 વપરાશકર્તાએ અજાણ્યા ઇ–મેઇલ એડ્રેસ પરથી મળેલ ડોક્યુમેન્ટ ડાઉનલોડ કરતા સમયે યોગ્ય સાવધાની રાખવી કારણ કે તેમા વાયરસ કે અન્ય માલવેર હોઇ શકે છે.

9.6 વપરાશકર્તા/વિભાગે GSWAN/સરકારી નેટવર્કમાંથી અસરગ્રસ્ત ઉપકરણ (કોઈપણ વાયરસ/માલવેર/રેન્સમવેર વગેરે) દૂર કરવું અને આવા ઉપકરણનો અહેવાલ GSDC સુરક્ષા ટીમને ઇ–મેઇલ એડ્રેસ: incident-certg@gujarat.gov.in પર મોકલવો.

9.7 વિભાગની માલિકીની કોમ્પ્યુટર સિસ્ટમ્સ સોફ્ટવેર અને ઓપરેટિંગ સિસ્ટમના લેટેસ્ટ/સપોર્ટેડ વર્ઝન અને એન્ટી–વાયરસ સોલ્યુશન ઇન્સ્ટોલ સાથે અપ ટુ ડેટ રાખવામાં આવે છે કે કેમ તે વિભાગ/ખાતાના વડાએ સુનિશ્ચિત કરવાનું રહેશે.

9.8 https://gswan.gujarat.gov.in પર ઉપલબ્ધ એન્ટિવાયરસ સોફ્ટવેર માર્ગદર્શિકાની સૂચનાઓનું પાલન કરવું.

10. ઇન્ટરનેટ વપરાશ

નીચેની ગેરકાયદેસર પ્રવૃત્તિઓ પરત્વે કર્મચારીઓએ જાગૃત રહેવાની જરૂર છે;

10. 1 અશ્લીલ સામગ્રીની માલિકી રાખવી, ડાઉનલોડ કરવી અથવા તેનો પ્રસાર કરવો.

10. 2 કોમ્પ્યુટર સિસ્ટમનો અનઅધિકૃત રીતે એક્સેસ કરવો.

10. 3 નેટવર્ક સુરક્ષાને બાયપાસ કરવાનો પ્રયાસ કરવો.

10. 4 નુકશાન પહોચાડવાના ઉદ્દેશ્ય સાથે કોમ્પ્યુટર વાયરસનો ફેલાવો કરવો.

10.5 અધિકૃત યુઝર્સના ડેટા ઍક્સેસને બ્લોક કરવાના હેતુથી પરવાનગી વિના ડેટા ડીલીટ કરી નાખવો, મોડીફાય અથવા એન્ક્રિપ્ટ કરવો.

10.6 અધિકૃત યુઝર્સને પોતાના ડેટા અને કોમ્પ્યુટરનો ઉપયોગ કરવામાં અવરોધ ઊભો કરવો.

10.7 લોકોને તેમની સલામતી અથવા તેઓ જાણતા હોય તેવા કોઈપણની સલામતી માટે ભયભીત કરે તેવા અનઅધિકૃત ઈલેક્ટ્રોનિક મેસેજ મોકલવા.

10.8 નફરત અથવા હિંસા ઉશ્કેરતા સંદેશાઓ ઇન્ટરનેટના માધ્યમથી ફેલાવવા.

10.9 ઈલેક્ટ્રોનિક મેઇલ અથવા અન્યની ખાનગી વાતચીતને ઇન્ટરસેપ્ટ કરી સાંભળવી અને અટકાવવી.

10.10 કૉપિરાઇટનું ઉલ્લંઘન કરવું.

10.11 કોઈની પ્રતિષ્ઠાને નુકસાન પહોંચાડી શકે તેવી અફવાઓ અથવા આરોપો જેવી ખોટી માહિતી ફેલાવવી.

10.12 ઈલેક્ટ્રોનિક રેકોર્ડ્સનો અનઅધિકૃત રીતે નાશ કરવો, ફેરફાર કરવો અથવા બનાવટી ઈલેક્ટ્રોનિક રેકોર્ડ ઊભો કરવો.

11. આધાર વપરાશ અંગેની માર્ગદર્શિકા

11.1 આધાર અધિનિયમ, ૨૦૧૬ અને તેના નિયમો કાળજીપૂર્વક વાંચવા અને આધાર અધિનિયમ, ૨૦૧૬ અને તેના નિયમોની તમામ જોગવાઈઓનું પાલન સુનિશ્ચિત કરવું.

11.2 સંપૂર્ણ આધાર નંબર ડિસ્પ્લે માત્ર આધાર ધારક અથવા એજન્સી/વિભાગમાં જરૂરિયાત ધરાવતા વિવિધ વિશેષ ભૂમિકાઓ/વપરાશકર્તાઓ માટે જ નિયંત્રિત હોવું જોઈએ. અન્યથા ડિફૉલ્ટ રૂપે, ડિસ્પ્લે કરવામાં આવતા બધા આધાર નંબર માસ્ક કરેલા હોવા જોઈએ.

11.3 માહિતી પ્રસારણ સ્ત્રોત (વેબસાઇટ, રિપોર્ટ વગેરે) UIDAI ની સુરક્ષા જરૂરિયાતોનું પાલન કરે છે કે કેમ તેની ચકાસણી કરવી.

11.4 કર્મચારીઓ અને અધિકારીઓ કોન્ફિડેંસીયાલિટી અને ડેટા પ્રાયવસી બ્રીચીસ અંગેની અસરોને સમજે છે તેની ખાતરી કરવી.

11.5 કોઈ આધાર ડેટા બાહ્ય એજન્સીઓ અથવા અનધિકૃત વ્યક્તિઓને પ્રદર્શિત અથવા જાહેર કરવામાં આવ્યો નથી તેની ખાતરી કરવી.

11.6 આધારનો ઉપયોગ કરતી તમામ એપ્લિકેશનો તેની ડેટા સુરક્ષા માટે STQC/CERT-IN જેવી પ્રમાણિત એજન્સી દ્વારા ઓડિટ અને સર્ટીફાઇડ કરાવવી.

11.7 આધાર ઓથેન્ટીકેશન માટે માત્ર STQC/UIDAI પ્રમાણિત બાયોમેટ્રિક ઉપકરણોનો ઉપયોગ કરવો.

11.8 સાર્વજનિક ડોમેન/વેબસાઈટ વગેરેમાં આધાર સહિત કોઈપણ વ્યક્તિગત ઓળખી શકાય તેવા ડેટાને પ્રકાશિત કરવો નહીં. આધારની વિગતોનું પ્રકાશન આધાર અધિનિયમ હેઠળ શિક્ષાપાત્ર છે.

11.9 પીસી, લેપટોપ, સ્માર્ટ ફોન, ટેબ્લેટ અથવા અન્ય કોઈપણ ઉપકરણો જેવા કોઈપણ અસુરક્ષિત એન્ડપોઈન્ટ ઉપકરણોમાં કોઈપણ આધાર આધારિત ડેટા સંગ્રહિત કરવો નહીં.

11.10 રેશનકાર્ડ/જન્મ પ્રમાણપત્ર/જાતિ પ્રમાણપત્ર/કોઈ અન્ય પ્રમાણપત્ર/દસ્તાવેજ જેવા અન્ય વિભાગીય ડેટા સાથે વ્યક્તિગત રીતે ઓળખી શકાય તેવા આધાર ડેટાને પ્રિન્ટ/પ્રદર્શિત કરવો નહીં. જો આધાર નંબર પ્રિન્ટ કરવો જરૂરી હોય તો, આધાર નંબર કટ કરવો અથવા માસ્ક કરવો જોઈએ. આધારના માત્ર છેલ્લા ચાર અંકો જ પ્રદર્શિત/પ્રિન્ટ કરવા જોઈએ.

11.11 આધાર સંબંધિત કોઈપણ માહિતી કોઈપણ બાહ્ય/અનધિકૃત એજન્સી અથવા વ્યક્તિ અથવા એન્ટિટીને જાહેર કરવી નહીં.

11.12 કોઈપણ અનધિકૃત લોકોને સંગ્રહિત આધાર ડેટા ઍક્સેસ કરવાની પરવાનગી આપવી નહીં.

નોંધ: UIDAI અથવા આધાર અંગે વધુ માહિતી માટે https://uidai.gov.in/ વીઝીટ કરવી.

12. GSDC ની બહાર હોસ્ટ કરેલ રાજ્યના IT એસેટ્સ

12.1 મહત્વપૂર્ણ સિક્યોરિટી સલાહ માટે SOC, GSDC, CERT-IN, NCIPC, NIC-CERT, OEM અને અન્ય એજન્સીઓ સાથે સંકલન કરવું અને સાયબર થ્રેટ્સથી બચવા માટે જરૂરી સક્રિય પગલાં લેવા.

12.2 તમામ સર્વર્સ, ક્લાયન્ટ મશીનો, વેબસર્વર, ડેટાબેજીસ વગેરે અને સુરક્ષા ઉપકરણો પર યોગ્ય સુરક્ષા હાર્ડનીંગ હાથ ધરવામાં આવેલ છે તેની ખાતરી કરવી.

12.3 જ્યાં લોગિંગ સપોર્ટેડ છે ત્યાં તમામ સર્વર્સ, નેટવર્ક અને સુરક્ષા ઉપકરણો, સ્ટોરેજ, VM અને અન્ય કોઈપણ ICT ઈન્ફ્રાસ્ટ્રક્ચર અથવા સેવાઓમાં લોગિંગ એનેબલ છે તે સુનિશ્ચિત કરવું.

12.4 મહત્વપૂર્ણ નેટવર્ક અને સુરક્ષા ઉપકરણોના લોગનું નિયમિતપણે નિરીક્ષણ કરવું.

12.5 હોસ્ટ કરેલ એપ્લીકેશન/વેબસાઈટનું સુરક્ષા ઓડિટ થયેલ છે કે કેમ અને HTTPS સાથે સિક્યોર થયેલ છે કે કેમ તેની ખાતરી કરવી.

12.6 જો ઈ–મેઇલ સેવાનો ઉપયોગ કરી રહ્યા હોય તો ઈ–મેઇલ ગેટવેએ SPF, DKIM, DMARC, SMTP થ્રોટલિંગ અને રિવર્સ DNS લુકઅપને એનેબલ કરીને ઈ–મેઇલ સ્પામિંગ, ફિશિંગથી સુરક્ષિત રાખવું.

12.7 જો તમારું પોતાનું DNS સર્વર હોય તો DNS Spoofing અને DNS poison રોકવા માટે BIND DNS સર્વર્સ પર DNSSEC લાગુ કરવું.

12.8 જો ફાયરવોલ વાપરી રહ્યા હોવ તો ફાયરવોલના બધા પોર્ટ ડિફોલ્ટ રૂપે બંધ રાખવાની પોલિસી લાગુ કરવી અને ચોક્કસ સોર્સ અને ડેસ્ટિનેશન વચ્ચે માત્ર જરૂરી પોર્ટ જ ખોલવા.

12.9 IPS, HIPS, AV વગેરેમાં નિયમિત રીતે સિગ્નેચર અપડેટ કરવા.

12.10 Windows સિક્યુરિટી પેચ અપડેટ કરવા. જો Linux સર્વર હોય તો એપ્લીકેશન ડેવલપિંગ એજન્સી સાથે પરામર્શમાં રહી પેચો અપડેટ કરવા જોઈએ. પેચિંગ માટે WSUS અથવા yum સર્વરનો ઉપયોગ કરી શકો છો.

12.11 થ્રેટ્સ શોધવા માટે તમામ ઇનકમિંગ અને આઉટગોઇંગ ઇમેઇલ્સને સ્કેન કરવા અને અંતિમ વપરાશકર્તાઓ સુધી પહોચતા પહેલા એક્ઝિક્યુટેબલ ફાઇલોને ફિલ્ટર કરવી.

12.12 એન્ટી વાઇરસ અને એન્ટી માલવેર સોલ્યુશન્સ આપોઆપ નિયમિત સ્કેન કરવા માટે સેટ કરેલ છે તેની ખાતરી કરવી.

12.13 પ્રિવિલેજ એકાઉન્ટના ઉપયોગનું વ્યવસ્થિત સંચાલન કરવુ. ઓછામાં ઓછા પ્રિવિલેજના સિદ્ધાંતનો અમલ કરવો. જ્યાં સુધી એકદમ જરૂર ન હોય ત્યાં સુધી કોઈપણ વપરાશકર્તાઓને એડમીન ઍક્સેસ સોંપવો જોઈએ નહીં. જેમને એડમિનિસ્ટ્રેટર એકાઉન્ટ્સની જરૂરિયાત હોય તેઓએ જ્યારે જરૂરી હોય ત્યારે જ તેનો ઉપયોગ કરવો જોઈએ.

12.14 રોજિંદી પ્રવૃત્તિઓ કરવા માટે હંમેશા નોન–એડમિનિસ્ટ્રેટર એકાઉન્ટનો ઉપયોગ કરવો.

12.15 ઓછામાં ઓછા પ્રિવિલેજને ધ્યાનમાં રાખીને ફાઇલ, ડિરેક્ટરી અને નેટવર્ક શેર પરવાનગીઓ સહિત ઍક્સેસ નિયંત્રણોને ગોઠવવા. જો કોઈ વપરાશકર્તાને માત્ર ચોક્કસ ફાઈલો રીડ એક્સેસની જરૂર હોય, તો તેની પાસે તે ફાઈલો, ડિરેક્ટરીઓ અથવા શેર્સની રાઇટ ઍક્સેસ હોવી જોઈએ નહીં.

12.16 ઈમેલ દ્વારા પ્રસારિત થતી Microsoft Office ફાઈલોમાંથી મેક્રો સ્ક્રિપ્ટ્સને ડીસેબલ કરવી. સંપૂર્ણ Office સ્યુટ એપ્લિકેશનને બદલે ઈમેઇલ દ્વારા પ્રસારિત Microsoft Office ફાઇલોને ખોલવા માટે Office Viewer સોફ્ટવેરનો ઉપયોગ કરવો.

12. 17 જો એપ્લિકેશન/વેબસાઈટ લોડ બેલેન્સર અથવા WAF પાછળ રાખવામાં આવેલ હોય તો X-Forwarded for (XFF) એનેબલ રાખવુ, જેથી મૂળ IP વેબ એક્સેસ લોગમાં કેપ્ચર થાય.

12. 18 સ્કેમ્સ, malicious લિંક્સ અને સોશિયલ એંજીન્યરિંગના પ્રયાસોને ઓળખવા માટે કર્મચારી શિક્ષણ કાર્યક્રમોનું આયોજન કરવું અને અમલ કરવો.

12. 19 વિન્ડોઝ આધારિત સર્વર્સમાં પાવરશેલ અને Linux આધારિત સર્વરમાં સુડોને ડીસેબલ રાખવું.

12. 20 ઓછામાં ઓછા અર્ધવાર્ષિક તમામ ઉપકરણોની નિયમિત VA/PT (વલ્નરેબિલિટી એસેસમેન્ટ અને પેનેટરેશન ટેસ્ટીંગ) કરવુ. આદર્શ રીતે, આને શક્ય તેટલી વાર VA/PT કરવું જોઇએ.

12. 21 તમારા બેકઅપ્સ યોગ્ય રીતે કાર્ય કરે છે તેની ખાતરી કરવા માટે બેકઅપ્સને રીસ્ટોર કરી ટેસ્ટ કરો.

12. 22 ખાસ કરીને નવા–રજિસ્ટર્ડ ડોમેન્સ માટે નિર્ધારિત તમામ આઉટબાઉન્ડ ટ્રાફિકનું મોનિટરિંગ અથવા "અવર્ગીકૃત" કેટેગરી સંબંધિત ટ્રાફિકનું ખાસ નિરીક્ષણ કરવું જોઈએ અથવા બ્લોક કરવો જોઈએ.

12. 23 એટેક્ સેનવાસને ઘટાડવા માટે જ્યાં પણ શક્ય હોય ત્યાં IP બ્લોકિંગ અથવા ભૌગોલિક સ્થાન પ્રતિબંધો લાગુ કરી શકાય છે.

12. 24 રિમોટ ડેસ્કટોપ, ટેલનેટ, SSH અને અન્ય કોઈપણ વહીવટી ઍક્સેસને ફક્ત VPN IP માટે જ મંજૂરી હોવી જોઈએ.

12. 25 Anydesk, Ammy Admin, Team Viewer જેવા કોઈપણ રીમોટ એડમિનિસ્ટ્રેશન ટૂલ્સનો ઉપયોગ કરવો નહીં.

13. સિક્યોરિટી એડવાઈઝરી અને ઈનસીડન્ટ રિપોર્ટિંગ

13. 1 DST (https://dst.gujarat.gov.in), NIC-CERT (https://niccert.nic.in) અને CERT-In (https://www.cert-in.org.in) દ્વારા પ્રકાશિત સુરક્ષા એડવાઈઝરીનું પાલન કરવુ.

13. 2 શંકાસ્પદ મેઈલ અને ફિશીંગ મેઈલ સહિત કોઈપણ સાયબર સુરક્ષા ઈનસીડન્ટની જાણ GSDC સુરક્ષા ટીમ (incident-certg@gujarat.gov.in)ને અને CERT-In (incident@cert.org.in)ને કરવી.

14. સાયબર સિક્યોરિટી સંસાધનો

ભારત સરકાર દ્વારા પ્રકાશિત સાયબર સુરક્ષા સંબંધિત સૂચનાઓ/માહિતી સંબંધિત વધુ વિગતો માટે નીચેના સંસાધનોનો સંદર્ભ લઈ શકાય છે:

Sr.	Resource URL	Description
1	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in	Security Tools & Best Practices
5	https://infosecawareness.in/	Security Awareness Materials
6	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips
7	https://dst.gujarat.gov.in	Law, Policies, Guidelines & Advisories
8	https://gswan.gujarat.gov.in	Security Tools, Guidelines & Advisories

15. ચીફ ઇન્ફોર્મેશન સિક્યુરિટી ઓફિસર (CISO)

સરકારી વિભાગ/કચેરીમાં નિયુક્ત ચીફ ઇન્ફોર્મેશન સિક્યુરિટી ઓફિસર (CISO) એ DST/DIT/GSOC દ્વારા નિર્દેશિત સાયબર સિક્યોરિટી કાર્યક્રમોના અમલીકરણ માટે જવાબદાર છે. તેઓ સાયબર સિક્યોરિટી પોલિસી, ગાઈડલાઇન, અને પ્રોસીઝરનું પાલન સુનિશ્ચિત કરે છે, કર્મચારીઓમાં સાયબર સિક્યોરિટી અંગે અવેરનેસ ફેલાવે છે અને સિસ્ટમ અપડેટ્સની દેખરેખ

રાખે છે. CISO સિક્યોરિટી એડવાઈઝરીઓ પર સમયસર પગલાં લે છે, નિયમિત સાયબર સિક્યોરિટી ઓડિટનું સંકલન કરે છે અને નવા ઈ–ગવર્નન્સ પ્રોજેક્ટ્સ શરૂઆતથી જ સાયબર સુરક્ષાને ધ્યાનમાં રાખીને તૈયાર કરવામાં આવે તેની ખાતરી કરે છે.

16. અનુપાલન

ગુજરાત સરકારના ટેમ્પરરી, કરાર આધારિત/આઉટસોર્સ સહિત તમામ કર્મચારીઓ/અધિકારીઓએ સાયબર સુરક્ષા માર્ગદર્શિકાનું ચુસ્તપણે પાલન કરવાનુ રહેશે તથા તેને સુનિશ્ચિત કરવાની જવાબદારી જે–તે વિભાગ/ખાતા/કચેરીના વડાની રહેશે. જો માર્ગદર્શિકા નું પાલન કરવામાં નહીં આવે તો સંબંધિત CISO/વિભાગ/HoDs/બોર્ડ/PSU/કંટ્રોલ હેડ હેઠળની સંસ્થાઓ દ્વારા કાર્યવાહી કરવામાં આવશે.

सत्यमेव जयते
ગુજરાત સરકાર
Government of Gujarat

Cyber Security Guidelines for Protecting State IT Assets

DEPARTMENT OF SCIENCE & TECHNOLOGY

(Circular No: DST/ADV/e-file/24/2024/0599/E-Governance, Date: 20/11/2024)

Department of Science and Technology
Government of Gujarat
Block no. -7/5, Saradar Patel Bhavan, Sachivalaya, Gandhinagar
Gujarat, India
Website: https://dst.gujarat.gov.in/

TABLE OF CONTENTS

- **ABBREVIATION**

GoG/state	Government of Gujarat
DST	Department of Science & Technology, GoG
GoI	Government of India
Meity	Ministry of Electronics & IT, GoI
GSWAN	Gujarat State Wide Area Network
GSDC	Gujarat State Data centre
OS	Operating System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secured
BIOS	Basic Input Output System
VPN	Virtual Private Network
USB	Universal Serial Bus
ICT	Information and Communication Technology
CERT	Computer Emergency Response Team
HoD	Head of Department
URL	Uniform Resource Locator
OEM	Original Equipment Manufacturer
UIDAI	Unique Identification Authority of India, GoI
GPS	Global Positioning System
NFC	Near Field Communication
AI	Artificial Intelligence
CISO	Chief Information Security Officer
DIT	Directorate of ICT & e-Governance
GSOC	Gujarat Security Operation Center

- **INTRODUCTION**

In this digital era, technology is evolving in various forms, like digital transformation initiatives, cloud computing, AI, and remote work. Technology is an enabler in creating ease of life and ease of doing business. Consequently, cyber threats and risk incidents have increased significantly worldwide. There is growing risk of cyber threats affecting IT networks, systems, and data, which can negatively affect e-governance and result in substantial costs.
This guideline has been prepared with the objective to create a safe and secure ICT environment in the state.

1. SCOPE

All Gujarat Government(GoG) Departments/Head of the Departments /Board/Public Sector Undertakings/Organizations under control and its officers/ employees (including outsourced/contractual employees) are required to adhered to this guideline.

2. DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE

2.1 Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work. If required admin access to be given to users with approval from appropriate authority.
2.2 Set BIOS Password for booting.
2.3 Ensure that the Operating System and BIOS firmware are updated with the latest updates/patches.
2.4 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.
2.5 Applications/software's, which are related to official work, shall be installed/used; any other application/software shall not be installed/used.
2.6 Desktop must be locked/logged off when workspace is unoccupied and must be shut down if not in use.
2.7 Keep Desktop/Laptop and printer's software updated with the latest updates/patches.
2.8 All printer trays and fax trays of machines should be cleared of papers as soon as they are printed. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
2.9 Setup unique pass codes for shared printers.
2.10 Internet access to the printer should not be allowed.

2.11 Printer to be configured to disallow storing of print history.
2.12 Enable Desktop Firewall for controlling information access.
2.13 Keep the GPS, Bluetooth, NFC and other sensors disabled on the desktops /laptops and mobile phones. They may be enabled only when required.
2.14 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.
2.15 Do not use any external Mobile App based scanner services (ex: Cam scanner) for scanning internal government documents.
2.16 Don't use pirated Operating systems and software/applications.
2.17 Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table) and also Don't share it with any unauthorized person.
2.18 Take regular offline backup of important data.

3. PASSWORD MANAGEMENT

3.1 Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
3.2 Use Multi-Factor Authentication, wherever available.
3.3 Users must use a separate, unique password for each of their work related accounts.
3.4 Don't save passwords, payment related information or any important data in the internet browser or in any unprotected documents.
3.5 Passwords must be kept secret and should not be shared.

4. INTERNET BROWSING SECURITY

4.1 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.
4.2 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.
4.3 Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
4.4 Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies etc).
4.5 Don't use any 3rd party toolbars & extensions/plugins (ex: download manager, weather tool bar, ask me tool bar etc.) in internet browser.

4.6 Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software's).

4.7 Don't use your official systems for installing or playing any Games.

4.8 Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/) or popup window. Many malwares and phishing sites abuse URL shortener services. Such links may lead to a phishing/malware webpage, which could compromise your device.

5. MOBILE SECURITY

5.1 Ensure that the mobile operating system is updated with the latest available updates/patches from trusted sources only.

5.2 Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.

5.3 Download Apps from official app stores of Google (for android) and apple (for iOS).

5.4 Don't accept any unknown request for Bluetooth pairing or file sharing.

5.5 Before installing an App, carefully read and understand the device permissions required by the App along with the purpose of each permission.

5.6 In case of any disparity between the permissions requested and the functionality provided by an app, users are advised not to install the App or deny for specific permission or allow while using the app only. (Ex: A calculator app requesting GPS and Bluetooth permission; There is no use of GPS & Bluetooth in calculator application. So, such type of permission is required to disable).

5.7 Note down the unique 15-digit IMEI number of the mobile device and keep it offline. It can be useful for reporting in case of physical loss of mobile device.

5.8 Use auto lock to automatically lock the phone or keypad lock protected by pass code/ security patterns/ Biometrics to restrict access to your mobile phone.

5.9 Use the feature of Mobile Tracking which automatically sends messages to two preselected phone numbers of your choice which could help if the mobile phone is lost/ stolen. Alternatively, you can use Find my Device functionality (if Available).

5.10 Take regular offline backup of your phone.

5.11 Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates.

5.12 Observe caution while opening any links shared through SMS, QR Codes or social media etc., where the links are preceded by exciting offers/discounts etc., or may claim to provide details about any latest news. Such links may lead to a phishing/malware webpage, which could compromise your device.

5.13 Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.

5.14 Disable automatic downloads in your phone.

5.15 Always keep mobile software updated from authorized OEMs.

6. E-MAIL SECURITY

6.1 Do not share the email password with any persons.
6.2 Don't use any unauthorized/external email services for official communication.
6.3 Don't click/open any link or attachment contained in mails sent by unknown sender.
6.4 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.
6.5 Disable automatically forwarding email to a third party email system.
6.6 Do not use official email id provided by Government for any personal usage.

7. REMOVABLE MEDIA SECURITY

7.1 Perform a low format of the removable media before the first-time usage(Ex. Portable Hard Disk, Pen drive, CD etc.)
7.2 Perform a secure wipe to delete the contents of the removable media.
7.3 Scan the removable media with Antivirus software before accessing it.
7.4 Always protect your documents with strong password.
7.5 Don't plug-in the removable media on any unauthorized devices.

8. SOCIAL MEDIA SECURITY

8.1 Limit and control the use/exposure of personal information while accessing social media and networking sites.
8.2 Always check the authenticity of the person before accepting a request as friend/contact.
8.3 Use Multi-Factor authentication to secure the social media accounts.
8.4 Do not click on the links or files sent by any unknown contact/user.
8.5 Do not publish or post or share any internal government documents or any information not intended for public on social media.
8.6 Do not publish or post or share any unverified information through social media.
8.7 Do not share the official email address on any social media platform.
8.8 To follow the guidelines to be issued by Department of Science and Technology from time to time.

9. ANTIVIRUS USAGE

9.1 User shall install enterprise grade endpoint antivirus solution of DST.

9.2 User can download the antivirus solution from https://gswan.gujarat.gov.in/.

9.3 User shall periodically run full scan on his/her computer using above antivirus.

9.4 User shall uninstall any other antivirus software installed on their system apart from above antivirus solution.

9.5 Users shall exercise due caution while opening e-mail attachments received from unknown senders as they may contain viruses or other malicious software.

9.6 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 e-mail address: **incident-certg@gujarat.gov.in.**

9.7 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.

9.8 Please refer to Security & Antivirus software guideline at https://gswan.gujarat.gov.in.

10. INTERNET USAGE

The following actions are illegal, so employees need to be aware of that;

10. 1 Owning, downloading, or disseminating obscene content.

10. 2 Taking advantage of computer systems without authorization.

10. 3 Attempting to circumvent the electronic network security features.

10. 4 Virus transmission with malicious intent.

10. 5 Erasing, changing, or encrypting data without permission with the intention of blocking access by those who legitimately need to access it.

10. 6 Obstructing others' access to and use of their data and computers legally.

10. 7 Sending unauthorized electronic messages that make people fear for their safety or the safety of anyone they know.

10. 8 Spreading messages that incite hatred or violence against recognizable groups.

10. 9 Intercepting electronic mail or private conversations of others while it is being sent.

10. 10 Committing a copyright violation.

10. 11 Spreading false information that could harm someone's reputation, such as rumours or accusations.
10. 12 Unauthorized destruction, alterations, or falsification of electronic records.

11. ADVISORY FOR AADHAAR USAGE

11. 1 Read Aadhaar Act, 2016 and its Regulations carefully and ensure compliance of all the provisions of the Aadhaar Act, 2016 and its Regulations.
11. 2 Full Aadhaar number display must be controlled only for the Aadhaar holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
11. 3 Verify that information dissemination points (website, report etc) should comply with UIDAI's security requirements.
11. 4 Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.
11. 5 Ensure no Aadhaar data is displayed or disclosed to external agencies or unauthorized persons.
11. 6 Get all the applications using Aadhaar audited & certified for its data security by appropriate authority such as STQC/CERT-IN.
11. 7 Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.
11. 8 Do not publish any personal identifiable data including Aadhaar in public domain/websites etc. Publication of Aadhaar details is punishable under Aadhaar act.
11. 9 Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones or tablets or any other devices.
11. 10 Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other certificate/document. Aadhaar number if required to be printed, Aadhaar number should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed.
11. 11 Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.
11. 12 Do not permit any unauthorized people to access stored Aadhaar data.

Note: For more details visit site of UIDAI at https://uidai.gov.in/

12. STATE IT ASSETS HOSTED OUTSIDE GSDC

12. 1 Co-ordinate with SOC, GSDC, CERT-IN, NCIIPC, NIC-CERT, OEMs and other agencies for critical security advisories and take necessary proactive measures to ward-off cyber threats.

12. 2 Ensure that proper security hardening is carried out on all servers, client machines, webservers, databases, etc and security devices.

12. 3 Ensure that logging is enabled in all servers, network & security devices, storage, VMs and any other ICT Infrastructure or Services, where logging is supported.

12. 4 Regularly monitor the logs of critical network and security devices.

12. 5 Ensure that hosted applications/websites should be security audited and deployed with HTTP-secured.

12. 6 If using e-mail service then e-mail gateway should protect e-mail Spamming, Phishing by enabling SPF, DKIM, DMARC, SMTP throttling and reverse DNS lookup.

12. 7 If your own DNS Server, then Implement DNSSEC on BIND DNS servers to prevent DNS spoofing and DNS poisoning.

12. 8 If using Firewall, then apply Firewall all Port denied policy and opened only required ports between particular source and destination.

12. 9 Regular Signature Updating of IPS, HIPS, AV etc.

12. 10 Window Security patches should be updated. If Linux server then update patches in consultation with application developing agency. You may use WSUS or yum server for patching.

12. 11 Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.

12. 12 Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.

12. 13 Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.

12. 14 Always use a non-administrator account for carrying out day to day activities.

12. 15 Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

12. 16 Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.

12. 17 If the Application/Website is behind a Load Balancer or WAF, then please ensure that X-Forwarded for (XFF) is enabled, so that the Original IP is captured in the web access logs.

12. 18 Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.

12. 19 Disable PowerShell in Windows based servers and sudo in Linux based servers.

12. 20 Run regular VA/PT (Vulnerability and Penetration Testing) of all devices, at least half yearly. Ideally, run these as often as possible and practical.

12. 21 Test your backups through restore to ensure they work correctly upon use.

12. 22 Monitoring all outbound traffic especially the traffic that is destined to newly-registered domains or belongs to the category: "Uncategorized" should be inspected closely or blocked.

12. 23 Where ever possible IP restriction or Geo-location restrictions may be applied to reduce the canvas of attack.

12. 24 Remote desktop, Telnet, SSH and any other Administrative Access should be allowed only for VPN IPs.

12. 25 Do not use any remote administration tools like Anydesk, Ammy Admin, Team Viewer etc.

13. SECURITY ADVISORY AND INCIDENT REPORTING

13. 1 Adhere to the Security Advisories published by DST (https://dst.gujarat.gov.in), NIC-CERT (https://niccert.nic.in) and CERT-In (https://www.cert-in.org.in).

13. 2 Report any cyber security incident, including suspicious mails and phishing mails to GSDC security (incident-certg@gujarat.gov.in) and CERT-In (incident@cert.org.in).

14. CYBER SECURITY RESOURCES

The following resources may be referred for more details regarding the cyber security related notifications/information published by Government of India:

Sr.	Resource URL	Description
1	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in	Security Tools & Best Practices

5	https://infosecawareness.in/	Security Awareness Materials
6	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips
7	https://dst.gujarat.gov.in	Law, Policies, Guidelines & Advisories
8	https://gswan.gujarat.gov.in	Security Tools, Guidelines & Advisories

15. CHIEF INFORMATION SECURITY OFFICER (CISO)

The Chief Information Security Officer (CISO) in a government department is responsible for implementing cybersecurity programs as directed by DST/DIT/GSOC. They ensure compliance with cybersecurity policies, promote awareness among employees, and oversee system updates. The CISO promptly addresses security advisories, coordinates regular security audits, and ensures new e-governance projects are designed with cybersecurity in mind from the start.

16. COMPLIANCE

All Gujarat Government (GoG) Departments/Head of the Departments/Board/Public Sector Undertakings/Organizations under control and its officers/employees (including outsourced/contractual employees) are required to strictly adhere to the guidelines mentioned in this document. Any non-compliance may be acted upon by the respective CISOs/Department/Head of the Departments/Board/Public Sector Undertakings/Organizations under control heads.