Information Technology Policy and Procedures
of
MOTOR VEHICLES DEPARTMENT

GOVERNMENT OF NAGALAND

CONTENT:

1. Introduction and policy statement

2. Scope

3. Responsibilities

4. Security

5. Software Protection

6. Physical access controls

7. User access control to the IT network drives

8. Disposal/reallocation of equipment

9. Security incident investigation and reporting

10. Disaster recovery and business continuity

11. Risk management

12. Auditors

13. Compliance

14. Review

15. Signatories

16. Appendix

1 Introduction and policy statement.

1.1 This document sets out the Information Technology (IT) Policy for Motor Vehicles Department, Nagaland, for the Development, Management and Protection of its IT systems and defining baseline responsibilities for IT security, equipment and file storage. "IT systems" refers to the Motor Vehicles Department's, IT network, hardware including portable media, system and application software, communication components including telephone and WAN systems, documentation, physical environment and assets.

1.2 This Policy covers the IT networks for the Motor Vehicles Department staff across all sites and other network required by the Department to manage Department's websites and publishing systems.

1.3 The equipments covered by this policy include:

i. Network Infrastructure – The equipment housed internally to provide the Motor Vehicles Department IT network, including servers, enclosures, racks, cabling, switches/Routers, wireless access points, firewalls, proxies, authentication systems and devices, NTEs and remote access systems.

ii. Desktops – Personal Computers (PCs) issued or provided to staff in the course of carrying out their duties.

iii. Laptops/Netbooks - Portable Personal Computers issued or provided to staff in the course of carrying out their duties.

iv. Smart phones - Digital communication devices issued or provided to staff in the course of carrying out their duties.

v. Desk/Conference Phones – Telephones/mobile phones/Voice Communication devices connected to the Network Infrastructure including desk telephones, conference telephones), analogue telephony adaptors, wireless phones (cordless).

vi. Media/Portable Media – Electronic Storage Devices such as DVDs, CDs, memory sticks and hard drives issued or provided to staff in the course of carrying out their duties.

vii. External Communications Infrastructure – Equipment used to connect Motor Vehicles Department to the external world including the Wide Area Network, telephone lines, mobile networks, Wi-Fi networks, leased lines, LES/WES/Ethernet first mile circuits, ADSL circuits, SDSL circuits, Broadband Fibre, MPLS, SD-WAN, 4G/5G and all related equipment and services.

viii. All related Facilities & Estates controlled IT media used in the Department's domain.

ix. This covers all IT installations or external projects or programmes adopted by the Department.

1.4 The objective of this policy is to ensure**: -**

i. That the confidentiality of data and information assets are protected against unauthorised disclosure and incidents are promptly reported (see section 9).

ii. That the integrity of data and information assets are protected from unauthorised or accidental modification.

iii. The availability and accessibility of IT systems as and when required by authorised user.

iv. Responsibility and accountability of every authorised user.

v. Ensure compliance with applicable cybersecurity, privacy, and data protection requirements.

vi. Ensure secure delivery of digital services to citizens and stakeholders.

1.5 This policy sets out the principles of IT security including the maintenance, storage and disposal of data and explains how they will be implemented by the Department to ensure that there is a centralised and consistent approach to IT security.

1.6 The policy aims to raise awareness of the importance and necessity of IT security in the conduct of day-to-day business.

1.7 The policy supports the Department business objectives of ensuring that the security, integrity and availability of IT systems are balanced against the need for authorised user to access systems and services. It will also help to protect data from misuse and to minimise the impact of service disruption by setting standards and procedures to manage and enforce appropriate IT security.

1.8 The policy supports the legal obligations of the Department in the maintenance of security and confidentiality of information in accordance with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. It shall further comply with the provisions of the Digital Personal Data Protection (DPDP) Act, 2023. The Department shall ensure that the collection, processing, storage, sharing, retention, and disposal of personal data are aligned with the requirements of the DPDP Act, 2023, and any rules, regulations, or guidelines notified thereunder.

2 Scope

2.1 This policy applies to all IT systems of the Department and those working at or for the Departments:

i. All authorised users of the Department including secondment from other organisations.

ii. Agency workers.

iii. Contractors, where they are directly using Department’s IT network.

3 Responsibilities

3.1 IT Hardware/Technical section is responsible for ensuring that:

3.1.1 Electronic filing systems and documentation are well maintained for all critical job functions to ensure continuity;

3.1.2 No unauthorised staffs are allowed access to any Department's IT systems in any location.

3.1.3 Named individuals are given assigned to specific computer systems according to their job function and role in accordance to the principle of least privilege;

3.1.4 Any electronic hardware of the Department is maintained, repaired or replaced as and when required.

3.1.5 Hardware assets registers are maintained.

3.1.6 All authorised users are instructed in their security responsibilities periodically.

3.1.7 The allocation/disposal/reallocation of all computer hardware and software to ensure best practice usage, value for money and that all data storage devices, including portable electronic media, are purged of sensitive data (such as confidential or personal information) before disposal or reallocation.

3.2 Procedures are implemented to prevent the Department from exposure to fraud, theft or disruption of its systems; these include segregation of duties, dual control and staff rotation in critical susceptible areas.

3.3 IT Software section has the following responsibilities: **IT (S) IT Software

Electronic filing systems and documentation are well maintained for all critical job functions to ensure continuity;

i. Day to day responsibility for the management and security of the systems, equipment and services laid out in section 1.3, with specific technical responsibilities being allocated across the team and to outsourced service providers.

ii. To make all users aware of this policy and to ensure that users understand and are able to abide by them when carrying out work on Department's behalf.

iii. Monitoring and reporting on the state of IT security within Motor Vehicles Department and across all Motor Vehicles Department systems.

iv. Developing and enforcing detailed procedures to maintain security access to all Motor Vehicles Department systems.

v. Ensuring compliance with relevant legislation, policies and good practice for all internal systems.

vi. Monitoring of actual or potential IT security breaches for all internal systems. And reporting to the appropriate people as need be.

vii. Maintaining an IT asset register (see section 5.1).

viii. Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence to the Department.

3.4 IT Administrator Section has the following responsibilities:

i. Day to day responsibility for the management and security of IT Infrastructure and systems, along with any externally hosted or supplied systems and services. Specific technical responsibilities will be allocated across the IT Operations teams and to outsourced service providers (if required).

ii. To ensure all Users and Systems comply with this policy and further directions that comply with this policy as issued by the Department from time to time

iii. Monitoring and reporting on the state of IT security within the Motor Vehicles Department IT systems for which they are responsible.

iv. Providing/collection of information on a timely basis from different team to maintain a single asset register for the Department.

v. Ensuring compliance with relevant legislation.

vi. Purchasing all computer equipment and software/license to ensure value for money, consistency and compliance.

vii. Monitoring for actual or potential IT security breaches within the Motor Vehicles Department IT systems for which they are responsible. And reporting to the appropriate authority as need be.

viii. Ensure any and all information as reasonably required by the Business Planning and Resources Director is provided to fulfil its compliance roles.

3.5 The IT (Human Resources /Training Section) is responsible for ensuring that:

i. All Motor Vehicles Department staffs sign confidentiality (non-disclosure) undertakings as part of their contract of employment, and any contactors, temporary staff (including agency staff) and secondees sign the Motor Vehicles Department's standard confidentiality undertaking before they are permitted to use the Department systems.

ii. IT Admin and IT (S) are both notified immediately via the Starters / Leavers / Changers process about changes to user permissions so that access to the IT network can be amended as appropriate. This may include any instance where a member of staff is temporarily suspended from their duties.

iii. New staffs are given basic user training in IT Security as part of their induction.

3.6 Users who do not have administration rights over their issued equipment are responsible for ensuring that:

i. No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote log-in data secure (except where necessary to disclose them to the IT Cell for administrative purposes) and to deny unauthorised third-party access to Motor Vehicles Department systems. This is particularly important for home workers and when using wireless networks.

ii. All reasonable care is taken to protect the security of IT equipment they are issued together with confidential data stored on it when taken outside secure offices.

iii. All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the Motor Vehicles Department IT Cell regardless of the working state of the equipment.

iv. All due skill, care and attention is taken to ensure that no virus, Trojan spyware or other malware is introduced to their equipment or Motor Vehicles Department systems.

v. All due skill, care and attention is taken to ensure that no configuration, miss-configuration or alteration to systems, software, equipment or infrastructure has a detrimental effect on the normal running, availability or stability of the Motor Vehicles Department IT Infrastructure as detailed in section 1.3.

vi. Contractors engaged by the Motor Vehicles Department are provided with and comply with this policy.

vii. Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimise the risks and impacts should a security breach or loss of that equipment occur.

viii. Actual or suspected security breaches are reported as soon as they arise.

ix. The equipment for which they are responsible for is only used for work purposes (no private use) and specifically their own job.

x. Only staff explicitly authorised by the IT Admin/Associate of the Motor Vehicles Department can dismantle, repair or alter the Motor Vehicles Department supplied equipment.

xi. Further advice is contained in Appendix A.

4 Security

4.1 Technical security measures will be put in place to protect the Motor Vehicles Department systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.

4.2 Contact will be maintained with the appropriate State and National organisation to ensure that the Motor Vehicles Department IT systems comply with State & National standards and best practice regarding IT security management is implemented.

4.3 Email and internet use will be governed in accordance to the Email Policy of Government of India.

4.4 Allocation of accounts to temporary workers using a generic username that cannot be mapped back to the user will not be allowed.

4.5 All relevant contracts with third parties will include standard Government practice clauses on information security. All central processing equipment, including file servers, will be covered by third party maintenance agreements.

4.6 All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the Motor Vehicles Department.

4.7 All IT equipment, including virtual systems/storage, will be uniquely identified and recorded.

4.8 Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking or eating is not permitted in these areas.

4.9 Records of all faults and suspected faults will be maintained.

4.10 All the Motor Vehicles Department laptops must be encrypted with access to the Motor Vehicles Department IT networks via using a strong authentication method.

4.11 Access to premise server/communications rooms will only be with the expressed permission of the Motor Vehicles Department IT admin section and accompanied by the appropriate representative.

4.12 Memory sticks and other portable media must be encrypted or have password protection when sensitive data is being transported outside secure offices.

4.13 To ensure maximum data security all critical data will be made secured by mirroring and backup intervention.

5 Software protection

5.1 Only licensed copies of commercial software or in house developed software are used by the Motor Vehicles Department. The Department's IT Cell will maintain a register of all commercial software, including all software licenses, to ensure that the Department complies with licence conditions and relevant law. Users must not install ANY externally developed software on the Department's IT equipment without prior approval of the HOD or IT Cell.

5.2 All users are reminded it is a criminal offence to make or use unauthorised copies of commercial software and that offenders may be liable to disciplinary action.

5.3 Software products required by any Section should be approved by the Motor Vehicles Department IT (admin) cell prior to purchase.

5.4 The Department will minimise the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software and ensuring firewall policies follow appropriate national guidelines. Users must report any detected or suspected

viruses, Trojan, spyware or malware on their computers immediately to the Motor Vehicles Department IT Cell for operations as appropriate.

6 Physical access controls

6.1 Physical access controls to secure areas will minimise the threat to the Motor Vehicles Department IT systems through damage or interference. The Motor Vehicles Department IT Cell will be responsible for access to all IT systems located in secure areas, with access being restricted using the principle of least privilege. An entry restriction system to the server/communications rooms at all premises will be implemented.

6.2 The server/communications rooms and store rooms for IT equipment will be locked at all times and the keys/codes held securely by the Motor Vehicles Department IT (Admin) cell.

6.3 Authenticated representatives of third-party support agencies or other parties will be given access through specific authorisation from the IT (S) or IT (H) and will be supervised by Motor Vehicles Department IT Admin representatives while on site.

6.4 No remote access to the Motor Vehicles Department's IT systems will be given to third parties at any time unless specific authorisation is received from the Motor Vehicles Transport Department/ IT Admin. Such access if granted must be supervised at all times.

7 User access control to the IT network drives.

7.1 User access to the IT network drives will be granted where access is necessary to perform the person's job following the principle of least privilege. Access will be modified or removed as appropriate when a person changes job or leaves the Department. It will be the responsibility of the HR section to notify the Motor Vehicles Department IT (Admin) and IT Cell immediately of any changes required to access controls, and procedures will be established between the three teams to ensure this happens.

7.2 For those with existing access to the IT network, requests to change access permissions should be made to IT network Team. These will be authorised by IT Admin who will, if necessary, check the requirement with the relevant Officer in charge.

7.3 No individual will be given access to the IT network unless properly trained and made aware of his or her security responsibilities.

7.4 Each member of the staff shall be provided with adequate digital storage space for official purpose only as determined by the Department from time to time. The Department reserves the right and authority to either increase or decrease the storage capacity based on operational requirements and resource availability. In accordance with Government policies, Government-approved cloud storage services shall be utilized, if and when necessary, to facilitate secure storage, access, and management of official data. Every User shall ensure that the allocated storage is used only for official purposes and managed responsibly.

7.5 'U drives' (Depts network storage drive) remain part of the Department IT systems and the Department has full rights of access to all data stored on its IT network. The content of U drives is not routinely monitored but the Motor Vehicles Department reserves the right to view

content if there are reasonable grounds for doing so; for example, to prevent fraud or suspected breach of the Motor Vehicles Department policies.

7.6 Users are not permitted to store entertainment files upon the Motor Vehicles Department IT systems. Files which have the same nature but are for work purposes must be notified to and approved via the Motor Vehicles Department IT Cell.

8 Disposal/reallocation of equipment

8.1 Equipment allocated to an individual user (including memory sticks) must not under any circumstances be reallocated within a Department (or any other user) and must always be returned to the Motor Vehicles Department IT Cell for reallocation to ensure correct management of sensitive data.

8.2 Obsolete, beyond repair, damaged, or non-repairable equipment no longer required for the business purposes of the Motor Vehicles Department shall be disposed of in accordance with the Guidelines for the E-Waste Policy notified by the Department of Information Technology & Communication vide Government of Nagaland Notification No. IT & C/15-15/19/102 dated 02/12/2019.

9 Security incident investigation and reporting.

9.1 The objective of security incident investigation is to identify detect, investigate and resolve any suspected or actual computer security breach.

9.2 A security incident may take place in spite of all precautions being considered and adopted.

9.3 Incidents should be notified to the Motor Vehicles Department, IT Admin, in accordance with Incident Reporting Procedure.

9.4 All users must report actual security breaches, or any concerns or suspicions about security breaches or lapses as soon as they arise.

9.5 All actual security incidents will be formally logged, categorised by severity and actions recorded by the Department's IT Cell and reported to the Motor Vehicles Department, HOD.

10 Disaster recovery and business continuity.

10.1 All business-critical data will be replicated between servers at relevant locations so that if the servers in one location become unavailable, access is automatically switched to the servers in another location.

10.2 All official data shall be "backed up" through secure and reliable backup mechanisms to ensure data availability and business continuity. The Department may utilize Government-approved cloud backup services, in addition to on-premises backup systems, wherever feasible and appropriate. Critical ICT infrastructure shall be equipped with suitable power backup systems, such as Uninterruptible Power Supplies (UPS), to safeguard against data loss or equipment failure during power interruptions, switchovers, or emergency shutdowns.

10.3 To minimise the risk to the Department's IT systems, robust disaster recovery plans will be put in place to ensure:

i. Identification of critical computer systems.

ii. Identification of areas of greatest vulnerability and prioritisation of key users and user areas.

iii. Agreement with users to identify disaster scenarios and what levels of disaster recovery are required.

iv. Development, documentation and testing of disaster recovery plans, including identifying tasks, agreeing responsibilities and defining priorities.

v. Recovery plans cater for different levels of incident, including loss of key user area within a building, loss of building(s), loss of a key part of the IT network, and loss of processing power.

vi. The existence of emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel) and actions to be taken to return to full normal service.

11 Risk management

11.1 The objective of risk management is to identify, counter and report on actual and possible threats to IT systems.

11.2 Significant IT risks will be included in the Motor Vehicles Department risk register and will be made available to the Audit Committee.

12 Auditors

12.1 A periodic security audit of the IT network, infrastructure, and software systems shall be conducted by agencies authorised and empanelled by the Government of India.

12.2 The implementation of the Motor Vehicles Department's IT policy and procedures will be subject to periodic review by both internal and external auditors and the subsequent recommendations will be agreed and action plans put in place and monitored.

13 Compliance

13.1 Breach of this policy may result in disciplinary action. Any breach of the law will be reported to the appropriate authorities.

14 Review

14.1 This policy will be monitored by the IT Cell of the Motor Vehicles Department and shall be reviewed at least once either in the beginning or end of the year.

15 Signatories

Name:

Designation:

Signed: _____ Date: _____

Name:

Designation:

Signed: _____ Date: _____

On behalf of Motor Vehicles Department Staff Representatives.

Appendix A
Good Practice Guide

i. Below is a summary of recommended Do's and Don'ts for all users of Motor Vehicles Department IT systems. It is intended to complement approved Motor Vehicles Department policies and support new information governance standards set by the Department.

   a. **Do** ensure you keep security in mind when working – If you have been sent a file or a web link, are you sure you can trust the person it came from, is this the type of thing they would normally send, does it 'feel right'? Remember, lots of spam and viruses sent impersonate the e-mail address of a real person, so the e-mail may not have been sent by the person you think. Lots of viruses move from machine to machine as hidden files on storage devices. Remember, only IT equipment issued, or approved, by the Motor Vehicles Department IT Cell should be used, except where personal PCs and laptops are used in accordance with the Home Working policy.

   b. **Do** report any errors or problems promptly – If you have an error or an issue, especially if it may be security related, please report it to the IT (S) quickly and with as much detail as possible. Reporting that you had a problem 3 days ago and you can't remember the error message makes it almost impossible to track and correct the problem. Reporting promptly with details of which system (e.g. terminal server, e-mail) was affected, the date and time the problem occurred and the specific error message or event makes it much easier to find and fix the problem, and get you working again.

   c. **Do** think about what you are saving and copying onto the network and in e-mail. Does the file need to be there? How big is it? If you are saving an attachment out of an e-mail, remember to delete the copy in the e-mail to save using up double the space. If you are copying data from a pen drive, why is this necessary? If it is only for your use, can it stay on the drive?

   d. **Do** take care of the equipment you are issued with, either permanently or on loan. Most of it is expensive and it may contain sensitive or confidential data.

   e. **Do** remember to return the equipment before leaving the Department. All data will be securely erased by the Motor Vehicles Department IT Cell. Please note that any personal data that has not been erased from returned equipment may be viewed by the IT Cell.

   f. **Do** keep passwords secure and never disclose them to anyone else. Passwords should ideally contain at least 9 characters Alphanumeric with a mix of letters and symbols in upper and lower case.

   g. **Do** keep portable media, especially laptops, taken outside the Motor Vehicles Department offices secure at all times. For example, do not leave them in boots of cars overnight, in overhead luggage racks or unattended in other insecure areas. Where possible carry IT equipment in anonymous cases without a

manufacturer's logo and avoid using laptops in public places where possible if confidential information may be visible to other people.

h. **Don't** connect any equipment (Laptops, USB devices including storage devices, networking equipment, 4G/5G cards etc.) to the Motor Vehicles Department IT systems unless it has been supplied or specifically authorised by the Motor Vehicles Department IT Cell. If in any doubt, confirm with the helpdesk before connecting anything.

i. **Don't** download any Software, Software updates, Installation Packages, or Executable files from the Internet or external storage devices (USB sticks, external hard drives, CD-ROM, DVD etc.) onto the Department IT systems unless specifically authorised by the Motor Vehicles Department, IT Cell.

j. **Don't** install any software on any the Motor Vehicles Department IT systems unless specifically authorised by the Motor Vehicles Department IT Cell. All software installs are normally carried out by the Motor Vehicles Department IT Cell and user installation of software is only authorised in special circumstances.

k. **Don't** download, upload, store, copy or distribute any materials, data or software of a pornographic, obscene, indecent, racist, defamatory, libellous, sexist, offensive or otherwise unlawful nature (other than for properly authorised and lawful research, for which written notification must be given to the relevant Director).

l. **Don't** attempt to circumvent the security and restrictions in place on the Motor Vehicles Department IT systems. These are in place to ensure a safe working environment for all staff and maintain the security and resilience of the Motor Vehicles Department network.

m. **Don't** leave portable media unattended in public places where there is a potential for opportunist theft or compromise (i.e. installation of a virus).

n. **Don't** connect any Department issued equipment or storage devices into another computer or network unless you are aware the network is correctly maintained and up to date Anti-Virus protection is in place. Viruses can be transferred using machines and storage devices connected to compromised computers or networks.

o. **Don't** use the Motor Vehicles Department network, including U drives, for the storage of music files, as these may breach copyright permissions. Private photographic and or video files should not be stored on U drives as they use up large amounts of space.

ii. For further information and advice please contact the Motor Vehicles Department, IT Cell.