**Notebook Security Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

**GENERAL GUIDELINES 4**

**CUSTODIAN AND USAGE OF NOTEBOOK 5**

***ENFORCEMENT 6***

#### GENERAL GUIDELINES

* 1. The guidelines below are for notebooks issued to one user or on a shared-usage-basis. They apply for issuance whether on temporary or permanent-basis.
	2. The notebook, together with its peripherals/accessories shall be deemed and implied as one complete entity governed by the guidelines below whenever the term “notebook” is mentioned. Personally owned peripherals/accessories must not be used on the organization’s notebooks.
	3. For custodian and usage of notebooks, the custodian-user is solely responsible for the safekeeping custodian and usage of the notebook issued to him/her through adherence to the laid down guidelines here.
	4. The notebook is to be used ONLY by the custodian-user whom it was issued to, unless approved by the Head of Department for a shared-usage-basis.
	5. The notebook shall be used only for the Organization’s business purpose or for work-related functions.
	6. The custodian-user shall be responsible in securing the content (files) of the notebook against information theft or misuse. He/She shall exercise discretion in encrypting the files as necessary if they are confidential. For this, the custodian-user shall obtain the necessary file-encrypting tools and training on its usage.
	7. The custodian-user shall also use the Power-On password protection feature in the notebook to enable him/her in securing the notebook against unauthorized access. He/She shall also enable the Windows’ screen-saver with password access to secure the information within in the event the notebook is left momentarily unattended.
	8. As the notebook is the responsibility of the custodian-user, the physical security of the notebook shall at all times be maintained and not to be left unattended, example, in the car boot.
	9. ***The custodian user is liable to compensate the Organization for the replacement cost of the notebook and its content if the notebook is stolen or lost.***
	10. In the event of the notebook is stolen or lost, the custodian-user should report it to the appropriate authorities (e.g. the police) and to Head of Department immediately.
	11. If there is no internal security or police report to substantiate a theft or lost of the notebook, it shall be assumed that the custodian-user had failed to exercise due diligence in securing the notebook and he/she shall assumed full responsibility.
	12. Any defects noticed on the notebook or its media content (files) by the custodian-user should be reported immediately to Head of Department. Delayed or non-reporting shall render the custodian-user bearing full responsibility for the defect, with liability to any replacement cost as determined by Head of Department.
	13. On termination in employment with the Organization, custodian-user must return the notebook to the Organization with its peripherals/accessories AND all its content (files) intact before his/her last day of departure. He/She shall also surrender to the Organization any password(s), pass phrase(s) or the encrypting/decrypting key(s), which are used in securing the notebook’s hardware or its content-files.
	14. Further, the custodian-user is required to sign the **Employee’s Notebook Acceptance/ Agreement Statement** in acknowledgement that he/she shall comply with the conditions laid down above. A duplicate of the signed-copy would be kept by the Head of Department for records.

#### CUSTODIAN AND USAGE OF NOTEBOOK

* 1. Seek authorization/security advice from Head of Department before installing new software. Do not install unauthorized or own software unless authorization is obtained as in above.
	2. Seek security/security advice from Head of Department before downloading software. Do not download software from the Internet, or other sites outside organization.
	3. Do not change the operating system (O/S) configuration unless prior authorization is obtained from Head of Department. Do not change the antivirus settings.
	4. Do not alter or add on peripherals (e.g. higher CPU, memory chip, or extra circuit boards) without authorization.
	5. When a notebook is connected into the Organization’s internal network (LAN), it will be considered as a "desktop" since its usage is same as a desktop. Hence, the "Desktop Policy", "Anti-Virus Policy", "E-Mail Usage Policy" and "Internet Usage Policy" apply (these can be viewed in the *Enterprise Portal*).
	6. For required repair/maintenance, send the notebook only to authorized vendor. When sending the notebook for maintenance, if possible, first transfer all sensitive/confidential data/files to another secured media (e.g. floppy, CDRW, another hard disk). Then use suitable utilities to completely delete/erase-sector the files to prevent unauthorized access.
	7. For data backup, both confidential and non-confidential files should be backed-up to removable media e.g. CDRW, zip-disk, floppy. Frequency of backup to be determined at discretion by users.
	8. For confidentiality reason, encrypt any files at one’s discretion with the installed encrypting tool (e.g. *Cryptext*, *Windows2000*’s native *Encrypting-File-System*, etc)
	9. Enable the Screen-Saver with password access control. Do not read or otherwise exposed sensitive or confidential information on public transportation or at public places.
	10. Ensure the installed anti-virus software’s configuration with auto-protect mode is not altered, and that its virus signature or pattern is updated. (If notebook is connected within Organization’s internal network, this should be automated; else the signature is to be manually updated through removable media e.g. floppy disk).
	11. Do not leave notebook unattended with a modem turned-on or communications software enabled. In the modem software, do not enable “password save” or “password remember” option.
	12. For luggage check-in at the airport, bring on the notebook as hand luggage. Do not check in as baggage to prevent theft or damage. When at the X-Ray/Metal Detector, ascertain first that it is not damaging electro magnetically/radiation before allowing the notebook to be screened.
	13. When not in use, place notebook in locked briefcase, or in a cabinet/ secured place when not carried with.
	14. In the event that this is not possible, it should be placed away from sight. Do not leave the notebook unattended.
	15. To avoid damage to the data content, do not place the notebook near any electrical appliance that generates strong magnetic field, e.g. electrical-motor, TV, refrigerator or large audio-speaker.
	16. For maintenance reason, try to keep/use notebook in low-moist and cooling environment. Do not keep/use notebook in moist, humid or environmentally unstable condition.
1. **ENFORCEMENT**

# All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.

# Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.

* 1. Organization’s staff must ensure that organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.
	2. Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.