

Acceptable Usage Guidelines

Ncell

Guidelines

Approved Date:- 05/12/2016

Ncell	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Guideline Name DOCID: GD-IT-IS-02

Copyright © Ncell. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior permission in writing from Ncell.

These trademarks are the intellectual property of Ncell and are protected by applicable legislation.

All other products or company names are used for reference only and may be proprietary to their respective hold

	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

i. Document Identification

Document Title and Version:	GD-IT-IS-02 Acceptable Usage Guidelines
Effective Date:	05-12-2016
Document Author:	Information Security Team
Owner:	CIO/Head of IT
Approved By:	CEO

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)

iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Function Heads
Informed	All Employees and External Parties

iv. Digital Signature

CEO

CIO/Head Of IT

v. Revision History


Ncell	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Rev	Date	Author	Description	Approved By	Initiated Date
0	05-12-2016	Information Security Team	Initial document	Simon Perkins	05-12-2016
1	02-10-2019	Information Security Team	Revised – Formatted, Aligned to existing processes	Vishal Mani Upadhyay	13-12-2019
2	26-12-2019	Tarani Prasad Chaudhary	Revised- Formatting/editing	Vishal Mani Upadhyay	26-12-2019
3	02-10-2019	Information Security Team	Added 5.3.vii.Store, send or distribute customer information, copyright material or other Ncell confidential information to any public email services or public storages not authorized by Ncell.	Vishal Mani Upadhyay	14-12-2021
4	13-12-2021	Tarani Prasad Chaudhary	Revised- Formatting/editing	Andy Chong	15-12-2021
5	28-08-2023	Information Security Team	2. Review changed from annual to once every two years, 5.2.x USB to be disabled by default added. Changed names of teams and added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
6	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
7	30-04-2024	Information Security Team	Re-branding	CIO/Head of IT	

Ncell	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

Document Control	1
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Responsibilities	5
5. Acceptable Usage Guidelines	5
5.1 General use and ownership	5
5.2 Ncell-issued Laptops and Workstations	6
5.3 Internet	6
5.4 Wi-Fi	7
5.5 Network and system activities	7
5.6 Emails	8
5.7 Usage of customer information	9
5.8 Copyright Infringement	9
5.9 Software Usage	9
5.9.1 Restriction on installation/uninstallation	9
5.9.2 Privileged utility programs	10
5.9.3 Duplication of licenses	10
5.9.4 Monitoring	10
6 Governance and Compliance	10
7 Associated Documents	10

	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

This document aims to provide a clear set of guidelines for acceptable and unacceptable use of Ncell's assets. The assets provided by Ncell are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

2. Review and Updating

This procedure shall be reviewed annually or whenever significant changes occur in the organization.

3. Scope

This document applies to all employees, contractors, consultants, third parties and their affiliates having access to Ncell's information assets regardless of work location and applies to all aspects of use of all resources.

4. Responsibilities

The IS MR is responsible for ensuring that the persons to whom this guidelines apply are aware of it. This may include, but is not limited to:

- i. providing access to a copy of the document, for example, on the intranet;
- ii. reminders of the need for compliance with the document; and
- iii. providing updates or developments of the guidelines.

It is the responsibility of all users to abide by these guidelines.

5. Acceptable Usage Guidelines

5.1 General use and ownership

- i. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their manager or the HR;
- ii. Employees are responsible for protecting any information used and/or stored on/in their Ncell accounts/systems which they have access to. Any equipment and accessories handed over (e.g. PCs, laptops) should be handled with due care ensuring the protection of information contained therein;
- iii. Employees will only use the approved software in their PC/Laptop. If any software is required for business purpose that is not listed in approved software list, employee is required to take prior approval for it;
- iv. Employees may report to their manager or send an email to infosec@ncell.com.np if they observe any weaknesses in information security;
- v. Preventing the misuse of the assigned Access Card / Visitor Card is the responsibility of the cardholder;
- vi. Third party employees/ contractors/ consultants/ vendors shall be allowed access to use Ncell's Information Systems for official use only after appropriate approvals. Such third parties should comply to Ncell's *Access Management Procedure* for access to Ncell's information systems.;
- vii. Employees should not leave printed documented at the printers unattended. The same shall be applicable for fax;
- viii. Ncell's Internal Audit team and other authorized persons reserve the right to audit networks and systems on a periodic basis to ensure compliance with Information Security Policy, guidelines, processes, procedures including Acceptable Usage Guidelines;
- ix. Users should report any security incidents as per the *Information Security Incident Management Procedure*;
- x. Users will not bring any personal media/software/devices for use on organization's computer systems without proper approvals. Further, users shall not be allowed to take computer media out of organization's premises without appropriate clearances; and
- xi. It is prohibited to install/configure software that provides services externally/internally in end-user computers in Ncell office network. Such services need to be placed in approved Data Centers.

Ncell	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

- xii. Ncell retains the right to monitor the information systems (system and network traffic) for security purposes. Ncell is not obliged to monitor the IT Equipment. User's activity is logged and logs shall be shared with HR/management as and when required


5.2 Ncell-issued Laptops and Workstations

- i. Laptops must not be left in an unattended car and when in transit in a car they must be locked in the boot;
- ii. Laptops must be properly securely stored when not in use;
- iii. Users must not keep their laptops in 'Hibernate' mode. They must be properly shut down (i.e. selecting shutdown from the operating system menu) when not in use and secured in a suitable locked cabinet within their place of work;
- iv. Any user who intends to leave a laptop/PC for any period of time must ensure that it is left in 'locked'. (by pressing 'ctrl + alt+ del' and choosing 'lock this computer or pressing windows key and 'L')';
- v. Only approved users with administrator privileges on their PCs will be allowed to –
 - a. Reinstall Licenses/ approved Software application for troubleshooting purposes
 - b. Execute Licensed/ approved Software application that doesn't run without Admin Privilege
- vi. Damage to (including suspected tampering) or loss of the laptop must be reported to the HR or IT Helpdesk team who will advise on the action that must be taken;
- vii. User shall not attempt to disable/alter the software/configuration of PCs/Laptops;
- viii. Ncell authorized personnel shall have unrestricted access to the PCs/Laptops for investigation/support purposes; and
- ix. Ncell reserves the right to disable USB and any other hardware/software components.

5.3 Internet

Users shall not attempt to use or allow Ncell's Internet Service to be used to:

- i. Engage in any activity that is illegal under local, state or international law;
- ii. Access or download unauthorized and non-business-related software, including games, games upgrades or related software;
- iii. Download, transmit, view or store material which could be considered as pornographic, vulgar or profane; insulting, defamatory or offensive to any individual or organization; and which could harm Ncell's status or reputation;
- iv. Use unapproved chat software (e.g.;IRC, MIRC, yahoo, messenger, msn messenger etc.). Approval must be taken for using unapproved chat software in case of any business requirement;
- v. Conduct an act of electronic harassment of any kind;
- vi. Store, send or distribute confidential information, copyright material or other content which is subject to third party intellectual property rights, unless users have a lawful right to do so;
- vii. Store, send or distribute customer information, copyright material or other Ncell confidential information to any public email services or public storages not authorized by Ncell.
- viii. Tamper with, hinder the operation of or make unauthorized modifications to any network or system;
- ix. Send or distribute unsolicited advertising, bulk electronic messages or overload any network or system;
- x. Access, monitor or use any data, systems or networks, including another person's private information, without authority or attempt to probe, scan or test the vulnerability of any data, system or network; and
- xi. Obtaining unauthorized access to or knowingly modifying information held on Internet resources;
- xii. Access to the Internet from Ncell's computers has been provided as a business resource. Inappropriate personal use will be treated as a disciplinary offence.
- xiii. Ncell reserves the right to monitor Internet traffic for the purpose of preventing any activity that may be illegal, unauthorized or harmful to the Company, its employees / contractors, customers or business partners.
- xiv. Ncell also retains the right to block access to any Internet web site/category of websites/online serves as it deems appropriate.
- xv. Ncell reserves the right to log all internet access through corporate internet facility.

	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

5.4 Wi-Fi

- i. Users shall not use Ncell Wi-Fi in a way that violates law or the established processes/ policies of Ncell;
- ii. Use of Wi-Fi is controlled by login with user name and password. Users are responsible for all activity conducted under their user name. Users are expected to take reasonable precautions to prevent unauthorized and/or abusive use by other individuals;
- iii. Ncell Wi-Fi connection is for official use only. Users shall not use Wi-Fi for any commercial purpose;
- iv. Users shall not attempt to deceive others about their identity in electronic communications or other network traffic;
- v. Users shall not use Wi-Fi connection to threaten, intimidate, or harass other individuals;
- vi. Personal wireless networks in Ncell are prohibited;
- vii. If Wi-Fi connection of a user sends disruptive signals, or violates any of the above requirements, it will constitute a violation of Ncell's Regulations and could result in administrative or disciplinary procedures; and
- viii. The Wi-Fi network connection may be subject to monitoring, with cause, for security, legal, or troubleshooting purposes. This may include monitoring for bandwidth usage, security related incidents, or a request from legal/law enforcement authorities. In addition, the Information Security Team reserves the right to scan the network to assist in identifying and protecting against exploitable security vulnerabilities (e.g., viruses or worms) in efforts to preserve network integrity. Information gathered in such scans will be used only for the explicit purpose of monitoring network security.

5.5 Network and system activities

Data on Ncell's network shall be the property of Ncell Pvt. Ltd. and any unauthorized access, copying, modification or destruction of the data is prohibited. All approved windows hosts used by the employee that are connected to the Ncell Internet/intranet/Extranet, shall be continually executing approved virus-scanning software.

The following activities are strictly prohibited:

- i. Port scanning or security scanning unless prior permission is sought from the Information Security Team or required as part of employees normal job duty;
- ii. User shall not attempt to connect to any server/network element that they do not have authority to access or needed to carry out their job functions;
- iii. Executing any form of network monitoring which will intercept data not intended for the employee's or contractor's host, unless this activity is a part of the employee's / contractor's normal job/duty;
- iv. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee/ contractor/ third party user is not an intended recipient or logging into a server or account that the employee/ contractor is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
- v. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
- vi. Revealing account password to others or allowing use of account by others. This includes family and other household members when work is being done at home;
- vii. Making copies of system configuration files for users' own, unauthorized personal use or to provide to other people/users for unauthorized use;
- viii. Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session via any means locally or via the Internet/Intranet/Extranet unless this activity is a part of the employee's normal job duty;
- ix. Circumventing user authentication or security of any host, network or account;
- x. Downloading, installing or running security programs or utilities which reveal weaknesses in the security of a system. For example, Ncell users shall not run password cracking programs VAPT

Ncell	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

tools etc. Network Security & Audit team responsible or any nominated person can do so for business purpose only;

- xi. Users with administrator privileges on their laptops or workstations will not be allowed to –
 - a. Reset the local Administrator account password;
 - b. Uninstall existing Ncell IT installed software;
 - c. Uninstall/disable Antivirus software;
 - d. Disable Windows Firewall;
 - e. Create/modify/removal any user accounts; and
 - f. Sharing the folder with all domain user permission.

5.6 Emails

- i. All messages generated by email shall be considered to be the property of Ncell;
- ii. Users shall safeguard their email account by creating strong passwords as per the Ncell's password requirements. Users should not disclose their password to anyone else under no circumstances;
- iii. The following activities are strictly prohibited:
- iv. Sending implied or explicit message which criticize other individuals or organizations;
- v. Sending or forwarding emails containing defamatory, offensive or obscene expressions;
- vi. Postings by employees from Ncell email address to any newsgroups, unless posting is in the course of business duties;
- vii. Making fraudulent offers of products, items, or services;
- viii. Any form of harassment via email, whether through language, frequency, or size of messages;
- ix. Unauthorized use, or forging, of email header information;
- x. Creating or forwarding "chain mails"; and
- xi. Knowingly distributing files that contain viruses, spyware, trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property.
- xii. Ncell reserves the right to filter emails as it deems as SPAM. SPAM filters shall be implemented for protecting against SPAM attacks.
- xiii. Users shall not use or allow their email/ internet service to be used for:
 - a. Sending multiple unsolicited electronic mail messages or "mail-bombing" - to one or more recipient;
 - b. Sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
 - c. Using redirect links in unsolicited commercial e-mail to advertise a website or service;
 - d. Using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients to conduct any of the prohibited activities under this guideline;
 - e. Falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
 - f. Using or distribute any software designed to harvest email addresses; and
 - g. Hosting any device or service that allows email to be sent between third parties not under Ncell's authority or control.
- xiv. Users can reduce the amount of Spam by following the below mentioned practices:
 - a. Use separate email addresses for different purposes, such as a personal email address for friends and family and a business email address for work;
 - b. Do not open emails from dubious sources
 - c. Do not reply to Spam or click on links, including 'unsubscribe' facilities, in Spam;
 - d. Do not accept Spam-advertised offers;
 - e. Do not post your email address on publicly available sites or directories. If you must do so, look for options, such as tick boxes, that allow you to opt out of receiving further offers or information.;
 - f. Do not disclose your personal information to any online organization unless they agree (in their terms and conditions or privacy policy) not to pass your information on to other parties; and
 - g. Report any Spam you receive to the Information Security Team.

Ncell	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

5.7 Usage of customer information

- i. Employees shall not share customer information (phone numbers, addresses, CDRs etc) with third parties;
- ii. There needs to be a valid business justification to access customer information;
- iii. Users are expected to respect the privacy of others. Any attempt to gain access to private information or passwords (via technological or social means) is prohibited. Any form of identity theft or the compromising of another individual's personal information is strictly prohibited;
- iv. Users in custody of personal information of employees/ customers shall not disclose the same to third party except if agreed through contractual agreements for business purposes. If Ncell consigns handling of personal data to a subcontractor, Ncell will select an entity that is deemed as handling personal data appropriately and manage the contracted entity as necessarily and appropriately so that entrusted data is under safe control;
- v. Employees shall not remove records containing personal information from the office unless it is necessary for the purposes of carrying out their job duties, post required approvals;
- vi. Paper records containing personal information should be securely packaged in folders to protect against disclosure/ theft;
- vii. Personal information should never be viewed on a laptop screen while travelling on public transportations;
- viii. Employees are prohibited from sending personal information by e-mail or fax unless it is necessary to do so for business purposes; and
- ix. Any breach of privacy or loss or theft of personal information should be reported immediately to the Information Security Team, who may launch an investigation, if necessary.


5.8 Copyright Infringement

- i. Ncell supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement;
- ii. Users shall not use Ncell's resources to copy, adapt, reproduce, distribute or otherwise make available to other persons any content or material (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and down loaded information) which is subject to copyright or do any other acts in relation to this copyright material which would infringe the exclusive rights of the copyright owner or any applicable law;
- iii. Users shall not transmit, distribute, download, copy, cache, host, or otherwise store any information, data, material, or work that infringes the intellectual property rights of others; and
- iv. Installation of unlicensed software is strictly prohibited. Disciplinary action shall be taken if unlicensed software is found on PC/laptop or any other company owned asset.

5.9 Software Usage

5.9.1 Restriction on installation/uninstallation

- i. Ncell will provide copies of legally acquired software to meet all legitimate needs in a timely fashion and in sufficient quantities for all of its computers. The use of software obtained from any other source could present security and legal threats to the company, and such use is strictly prohibited;
- ii. End users shall be prohibited from installing any new software or hardware and uninstalling existing software on any Ncell device, including desktop computers, servers, or portable computers, without prior approval. All new software not covered under the authorized software list must be approved before installation on information systems;
- iii. Software requests must first be approved by the requester's Department Head and ESPP Team; and then be honored to the IT Helpdesk; and
- iv. Software must be selected from an approved software list, maintained by the IT Helpdesk/ Information Security Team, unless no selection on the list meets the requester's need.
- v. No user/team in Ncell including the ESPP team shall uninstall security related software without explicit consent from the Information Security Officer. Such requests if any shall be routed through an approval process in Jira.

	Ncell	Classification: Internal
	Acceptable Usage Guidelines	Owner: CIO/Head of IT
		Effective Date: 05-12-2016
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

5.9.2 Privileged utility programs

Access to system utilities should be granted only to privileged users who are authorized and have a business case for accessing the specific system utility. If the utility supports different privilege levels, it should be ensured that the privilege level is set based on need to know need to do basis;

- i. The system utilities should be kept separate from other normal user utilities/ programs. At any point, a normal user should not be able to gain unauthorized access to any of the system utilities;
- ii. All default system utilities that are considered unnecessary installed during commissioning of a new information system should be deleted/ uninstalled;
- iii. Many equipment/ applications are provided with diagnostic ports for remote diagnostic/ maintenance tasks through system utilities. Access to such ports should be restricted only to authorized source;
- iv. If the system utilities are used for remote administration/ maintenance tasks, remote access should be limited from pre-defined IP / Host addresses.; and
- v. All changes and activities performed by privileged users using system utility needs to be logged and monitored.

5.9.3 Duplication of licenses

- i. Software shall not be duplicated, reproduced, or installed on more than one machine without prior written authorization of the ESPP Team;
- ii. If a software license states it is eligible and approved for multiple use, the following conditions must be adhered to:
 - a. Use of the software is limited to Ncell business; and
 - b. The software must be removed from the computer if the individual is no longer employed by Ncell.

5.9.4 Monitoring

- i. Ncell has the authority to uninstall any unauthorized software or hardware, if it is discovered
- ii. Ncell reserves the right to protect its reputation and its investment in computer software by enforcing strong internal controls to prevent the making or use of unauthorized copies of software. These controls may include periodic assessments of software use, announced and unannounced audits of company computers to assure compliance, the removal of any software found on Ncell's property for which a valid license or proof of license cannot be determined, and disciplinary actions

6 Governance and Compliance

- i. Exception management process shall be followed to raise the exception for this procedure.
- ii. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

7 Associated Documents

- i. Asset Management Procedure
- ii. Information Security Incident Management Procedure
- iii. Access Management Procedure