Aditya Birla Capital

INFORMATION SYSTEMS ACCEPTABLE USAGE POLICY

Version 1.0

Document Details	
Document Title	INFORMATION SYSTEMS ACCEPTABLE USAGE POLICY
Document Owner	Makesh Chandramohan
Document Author(s)	Kushal Jadhav
Document Code	ABC/RISK/IAUP05
Document Version No.	1.0
Document Approver	Makesh Chandramohan
Approval Date	20/06/2018

Version Control

Date	Modified by	Reviewed By	Version No.	Nature of Change
10/05/2018	Gopakumar Panicker/Kushal Jadhav	Makesh Chandramohan	1.0	Applicability changed to all ABC employees

8.5.3 Acceptable use of Assets

Employees and external party users using or having access to ABC's assets should follow the below mentioned acceptable usage controls associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility. Information Security Policy including the Acceptable use of assets shall be signed by all employees. Use of Company's resources should be for business purposes.

Parameters	Acceptable Use (Dos and don'ts)
Email Communication	• ABC's email system shall be used only for the conduct of its business. • IT Function should ensure that the email system is equipped with spam filter and content scanning software. • A mass email to all employees is restricted to authorized personnel. It is expected that the content of the mails is official and based purely on business needs. The individual sending the email should apply appropriate judgment to determine the sensitivity of the contents and its implications. • Users must avoid opening any file attached from an unknown, suspicious or untrustworthy source. • The sender of an email targeted to a large group should take full ownership and should not send emails on someone else's behalf.
Electronic Communication with vendors / third party	• Confidential or sensitive material must not be transmitted over the Internet or by any insecure means. • Email between ABC and vendors / third party must only be initiated or received via the Company's email facility. • Use of personal Internet email accounts for exchanging information with vendors / third party or for conducting business on behalf of the Company is prohibited unless approved by your business Information security Function.
Internet usage	• Users should also be aware that many web sites employ technologies (e.g., cookies, Java applets, ActiveX components) may be designed to enable interactivity, track user preferences, or gather personal information. When a particular function of the web page is accessed, these Java applets or ActiveX components should be avoided.

Parameters	Acceptable Use (Dos and don'ts)

	• Authorized Users are responsible for ensuring that they never connect to the Internet [by modem/ Data Card] via an ISP without first disconnecting from ABC's network.
	• Do not retrieve information that might be considered offensive and avoid accessing Internet sites where such information is known to be published.
	• Restricted sites may include sites which contain:
	  ○ Sexually or radically offensive material
	  ○ Web based e-mails and message boards
	  ○ Terrorism related websites
	  ○ Sites distributing pornography, illegal goods and software, hacking tools, pirated material
	  ○ Popular websites of non-business nature which may lead to high utilization of bandwidth and restrict legitimate business use of the available bandwidth
	  ○ Sites that allow users to engage in personal discussions, posting of personal profiles, engaging in any kind of trading / e-commerce, auctions etc.
	  ○ Anti-national, anti-social content
	  ○ External proxy / Anonymous proxy
	• Do not download executable files without consulting IS Function. Executable files (e.g. shell scripts) may be 'Malwares' containing commands designed to corrupt the system or to weaken security.
	• Updates, service packs and patches to various licensed and/or ABC/Business IS approved software shall be installed only by your IT Function, either manually or automatically. Employees should not manually download such updates which may put their systems and client data at risk.
	• End-User shall not have any local admin rights on their laptop/desktop to install and uninstall software or make any change in configuration settings.
	• Business-related software should be installed by your IT Function by ensuring:
	  ○ It is appropriately verified and authenticated.
	  ○ It has been researched to determine the conditions required for its use (including shareware fees) and those conditions have been met.
	  ○ It has been scanned for viruses using the most current version of ABC standard anti-virus software.

Parameters	Acceptable Use (Dos and don'ts)
	○ ABC or your business has valid license to use it or the software usage does not require any license.
User ID and Password security	• All employees must use only those IDs that have been assigned for their use. Accessing ABC's computer systems, networks or applications using another employee's ID is strictly prohibited. • Employees must immediately report any instances of requests to use IDs other than their own, to Information security Function. • Each employee is responsible for all transactions made under the authorization of his/her system account. Hence users must choose a "complex" password that would be difficult to guess or crack. • Choose passwords, which are different from your previous passwords. • Passwords must never be printed, stored online, put on display boards or "Post-it notes", or shared with others. • Two-factor authentication devices should be kept securely and should not be left unattended.
Desktop and Laptop Usage	• Employees shall not install any software (whether freeware or licensed) without the knowledge of your business IT Function. • Uninstalling or stopping critical system processes/software, such as anti-virus, backup agent or policy enforcement software, is strictly prohibited. The absence of any such software should be reported immediately to your business IT/IS Function. • Users are responsible for protecting any information used and/or stored on/in their workstations. • Users should report any weakness in computer security, any incidents of possible misuse or violation of this policy to his/her manager or your business IT/ IS Risk management. • Users are prohibited from storing, transmitting or synchronizing any group or corporate information with their handheld devices unless the same is authorized. • Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright. Wherein copyright owner refers to the person or entity which possesses the exclusive right to make copies, license, and otherwise exploit a literary, business, musical, or artistic work, whether printed, audio, video, etc.

Parameters	Acceptable Use (Dos and don'ts)
	• Users shall not make copies of system configuration files for their own personal use or to provide to other people/ users for unauthorized use. • Users will not bring any personal media/software for use on ABC's computer systems. Further, users would not be allowed to take computer media out of ABC's premises without appropriate clearances. • Employees should ensure that they have the latest anti-virus signature files installed on their computer. If they suspect infection by a virus, they must immediately stop using their computer, disconnect from all networks and notify your business IS and IT Function. • All portable electronic media (USB drives, CD / DVD) must be scanned for viruses before use on ABC systems. • Report any malware or suspected occurrences to the IT Function. • File sharing with other users, if required, should always be carried out with password protection. • Employees are encouraged to properly log out and power off their systems when not in use or when they leave for the day. Apart from protecting against unauthorized usage of systems, such a practice also helps to keep systems updated with the latest patches and updates because many of these require a restart. • Executing any form of network monitoring, port scanning or network sniffing is strictly prohibited and would invite strict disciplinary action. • Users must not disable the pre-configured, password protected screensaver.
Laptop Protection	• Laptops should be kept with yourself securely. • Do not place heavy objects on the laptops. • Never check laptops as baggage. If the security wants to see it operate, make sure you are the one handling it. • Quit programs prior to shutting down. • Always transport your laptops in a sturdy weatherproof padded bag. • Do not allow any liquids to spill onto your laptops. • Do not place your laptop closer than 13cms from any electrical appliances that generate strong magnetic fields such as TV or change speakers. • Do not hard mount your laptop in a vehicle or anywhere that is subject to strong vibrations. • Do not keep your laptop inside a car in such a way that it is clearly visible from outside, even with the glasses closed. Keep it in the boot if you are leaving your car for a long time.

Parameters	Acceptable Use (Dos and don'ts)
	• Do not place any objects between the keyboard and display. • If the laptop is not going to be in use for more than a month, it is recommended that the battery be removed and stored in a cool clean dry place. • The concerned staff must file a police report immediately in the event a laptop is stolen or lost. The staff must also notify his/her manager or the respective IT head, within one business day of the theft/loss.
Physical Security	• Employees are required to always wear and display a visible identification (badge) while working in ABC's premises. • Access cards issued to employees must never be shared with other individuals. For safety and security reasons, tailgating is prohibited. Tailgating is following another person through a badge access point without using one's own badge. • Fax and Print-outs must be removed from fax machines and printers promptly. Unclaimed prints must be securely disposed-off using a shredder. • Employees must lock or log out of their workstation when they temporarily leave their desks.
Work Area/ Cafeteria	• In work premises where there is availability of dedicated lunch room / cafeteria, employees shall avoid consuming eatables and drinks in the areas housing Information Systems in order to avoid threats related to rodents. • Smoking and consumption of alcohol is strictly prohibited inside the premises.
Clear Screen & Clear Desk Policy	• Ensure that your screen is locked, whenever you leave your workstation by using 'Ctrl' + 'Alt' + 'Del' + 'Enter' • Clear your desks before leaving. Keep confidential information in secure storage. Keep filing cabinets shut and locked, when unattended. • Information should never be left lying around on unattended printers or fax machines. Empty in-trays and clear your work area before leaving it. • In case documents containing sensitive information are no longer required, they should be shred (or torn into small pieces), before disposal.
Mobile devices	• Employees shall be allowed to remotely connect to the ABC network using mobile computing device to access the business information, only after successful identification and authentication. • Employees are required to take special care of the mobile computing resources such as, but not limited to, laptops, mobile phones, handheld computing devices etc. that are issued by ABC, to prevent any compromise and/ or destruction of business information.

Parameters	Acceptable Use (Dos and don'ts)
	• Devices authorized for carrying out activities of Business/ Unit shall not be used for the purpose of illegal transactions like fraud; and obscene behavior like pornography, hate crimes, racial abuse, outside business activities, political activism etc. • The mobile devices need to be physically protected against theft. Insurance or other security requirements for laptops should be present in case of theft or loss. • The mobile devices which have confidential information should not be left unattended. • Mobile devices used for accessing ABC information and information systems shall be governed by information security policies and guidelines. It shall be responsibility of the employee to ensure that the mobile devices and their use are in compliance with these policies. • User must immediately report the loss/theft of tablets/smartphones/Laptops, used to access ABC information, to your business IT/IS Function. • Employees using ABC mails on their handsets must secure their handsets by use of automated locking (time out-max 5 minutes) and must require a password / PIN to unlock the same. • It is required that the user accepts updates of the Blackberry and other tablet/smartphone handheld software. • Users must consult with their business IT/IS Function for secure mail service use on their handheld devices. (Active-Sync and MDM).
Wireless Network Access	• Access to ABC WiFi network is restricted only to authorized ABC assets. No personal devices are allowed to be connected to ABC Wifi Network without expLICIT approval from your business CISO or ABC IS Function • Use of utilities like scanners, Wifi Packet capture softwares etc. is strictly prohibited • Guest Wifi access may be provisioned on case to case basis post approval from Business IS/ABC IS Function
Social Media	• Posting propriety and confidential ABC materials prohibited on all channels • Malicious opinions about the company or other employees must be kept out of public social networks • All associated individuals must be mindful of the customers' and employee privacy and must not post any related information on personal networks • All personal accounts of ABC employees should clearly mention that all posted opinions/content/creative are personal • Adhere to the controls mentioned in ABC Social Media Policy

Appendix A

Information Systems Acceptable Use Agreement

I/We have received a copy of Aditya Birla Capital's (ABC) Information Systems Acceptable Use Policy dated 20th June, 2018. I/We have read the aforementioned document, understood the same and agree to follow all policies that are set forth therein.

I/We recognize and understand that ABC's Information Systems, e-mail and Internet systems are to be used for conducting the ABC business only. I/We understand that use of this facility for private purpose is not allowed, except when expressly permitted. I/We am/are aware that ABC may access and review any materials stored on my/our workstation(s), handheld devices, USB or any other storage devices etc., or information sent or received by me/us through the ABC and/or Aditya Birla Group (ABG) network, e-mail or Internet connection.

I/we understand that this Acceptable Use Policy applies to me/us, and I/We am aware that violations of this policy may subject me/us to disciplinary action, up to and including termination from employment/of contract and / or any legal action.

I/We indemnify ABC, its Officers, and other employees of any damage, harm, and liability arising out of breach of this policy by me/us or due to any negligence on my/our part.

Furthermore, I/We understand that this policy document can be amended at any time by ABC. I/We further acknowledge that any changes in future to this policy may be communicated to me/us by displaying the same on notice board and / or by e-mail.

_____ _____

User Signature Date

_____ _____

User Name Employee Emp ID