




## Information Security

<b>Policy title</b>	Information Security
<b>Policy number</b>	IT.003
<b>Policy status</b>	Revised
<b>Version number</b>	7.0
<b>Policy effective date</b>	May 01, 2016
<b>Last reviewed on</b>	December 22, 2022
<b>Next review date</b>	December 21, 2024
<b>Business   Unit</b>	IT Unit
<b>Department   Function</b>	IT Infrastructure

	<b>POLICY</b>	Page #	2 of 8
		Revision number	7.0
	<b>INFORMATION SECURITY</b>	Effective Date	May 01, 2016
		Last reviewed on	December 22, 2022
		Next review date	December 21, 2024

## 1. OBJECTIVE:

The aim of this policy is to provide guidelines for ensuring the protection of Information that is stored on the end user devices | servers or in Transit.

## 2. SCOPE and ENTITLEMENT:


This policy would be applicable to all the employees and IT Systems administrators, who handle computer systems and Data.

## 3. RESPONSIBILITY:

President – IT (CISO) would be responsible for the effective administration of this policy.

## 4. GUIDELINES:

- 4.1. Information stored on servers and storage devices at company datacenters as well as on end user machines are of utmost importance. The data is also required to be protected while in transit through computer networks. This document provides the guidelines and processes that are in place to ensure Confidentiality, Integrity and Availability of digital information.
- 4.2. IT Administrators are responsible for ensuring the confidentiality of Information that is stored on Server and Storage Infrastructure.
- 4.3. Network Administrators are responsible for ensuring the security of data when it is transmitted over the wireless and wired network of the company. They need to protect the information assets of the company from outside threats (Internet) and inside threats (from disgruntled employees or exploited computers).
- 4.4. Users handling IT equipment like Desktop | Laptop | Handheld devices are responsible to ensure the security of both the device and data through the use of passwords and following the relevant guidelines provided by the IT unit. They are also required to refrain from sharing confidential information with other persons when under employment and even after their separation from the company.
- 4.5. Contractors and Data Entry operators hired by the company are also required to follow the information security guidelines and are responsible for maintaining

	<b>POLICY</b>	Page #	3 of 8
		Revision number	7.0
	<b>INFORMATION SECURITY</b>	Effective Date	May 01, 2016
		Last reviewed on	December 22, 2022
		Next review date	December 21, 2024


secrecy of information shared with them during and after their association with the Organization.

- 4.6. Information security awareness training will be imparted to the end users from time to time; all employees are required to attend the same. Training to new employees will be provided during induction programs.

## 5. PROCEDURE:


### 5.1. GENERAL:

- 5.1.1. Security controls and account privileges for the servers should be governed by specific SOPs viz. Server Administration, Logical Access Management and Password Management.
- 5.1.2. Sessions, which remain idle, needs to be terminated as per security best practice guidelines, all systems have such controls configured. For Oracle EBS, the idle session time out is set to 15 minutes.
- 5.1.3. Security configuration documents and advisories published by software OEMs from time to time.
- 5.1.4. Datacenters should be physically secured with biometric access control systems and the access to be governed as per Datacenter Operations SOP.
- 5.1.5. Data communication through Wireless computer networks should be encrypted and only authenticated users should be allowed access of wireless network.
- 5.1.6. Computer networks should be protected from external threats by use of Unified Threat Management system. Internet access should be controlled and should be compliant with the Corporate Internet Access Policy.
- 5.1.7. Intrusion detection and prevention system should be implemented to protect unauthorized access of computer networks and to prevent any data loss.
- 5.1.8. End user computing equipment's should be protected from Viruses and Malwares using Endpoint security software and such protection should be monitored on regular basis so as to ensure trouble free operations and

	<b>POLICY</b>	Page #	4 of 8
		Revision number	7.0
	<b>INFORMATION SECURITY</b>	Effective Date	May 01, 2016
		Last reviewed on	December 22, 2022
		Next review date	December 21, 2024

prevent to data loss.

- 5.1.9. End users must ensure confidentiality of their login credential and should not share the same with anyone. Such passwords forms the first line of defense and it is necessary that the passwords meets the complexity requirement as mentioned in password policy and controlled through active directory group policy.
- 5.1.10. End users are expected to lock their devices when not in use and should not leave them open in order to prevent unauthorized access of Information.
- 5.1.11. In case of printing sensitive information, user should use the printers providing password protected print feature or should ensure that the prints are collected from printers immediately after printing in order to ensure confidentiality of the Information.
- 5.1.12. Handheld devices must have the pass code (PIN) or pattern set in order to protect against misuse. Such pass codes (PIN) or Pattern should not be shared with anyone. In order to separate corporate data from personal data and to centrally administer such hand held device Mobile device management software should be deployed.
- 5.1.13. The required access of business application should be given after having the approval from the designated business owner in line with the Application Change management process.
- 5.1.14. HR should provide employee separation notification to IT as soon as the employee separate from the company. IT administrator should ensure to revoke the account privileges in a time bound manner.
- 5.1.15. In the event of a breach happening on account of non-adherence to the guidelines mentioned in the policy document the user accounts of concerned user | group of users responsible for such a breach will be suspended on immediate basis and their access to the compute device as well as business applications will be denied. HR unit in accordance with the "Code of Conduct" Guideline takes a final decision. If the offender is an external entity, our legal


	<b>POLICY</b>	Page #	5 of 8
		Revision number	7.0
	<b>INFORMATION SECURITY</b>	Effective Date	May 01, 2016
		Last reviewed on	December 22, 2022
		Next review date	December 21, 2024

department will be requested to take appropriate action as applicable. Business unit will be responsible to ascertain the Business Impact of such a breach and IT unit will provide the relevant system and audit logs as required by the Business function or HR.

- 5.1.16. Security breach will be recorded by IT unit as an Incident and necessary counter measures or process changes will be identified and put forward for management approval. Upon approval the same will be deployed in order to prevent recurrence of such breach in future
- 5.1.17. IT team in consultation with HR will plan and organize security awareness training for users.
- 5.1.18. IT managers handling the information management system will be encouraged to attend training programs | webinars organized by security solution providers in order to hone their skills and for continuous update of their Information security knowledge.

## 5.2. EMAIL SECURITY:

- 5.2.1. 2GB mailbox will be provided by default, 4GB mailbox will be provided to Business Head.
- 5.2.2. User is required to routinely archive the old mails in order to remain within the allotted quota of 2 GB.
- 5.2.3. In exceptional cases if it is a must to have higher storage quota, user is required to take email approval from their respective Business | Unit head and submit the request to admin@atul.co.in , such request will be submitted to IT unit head for approval and upon approval the mailbox quota will be raised in incremental steps of 2 GB.
- 5.2.4. Attachment Size is restricted to 10 MB for external domains and 25 MB for internal communication.
- 5.2.5. Third party Mail filtering service has been deployed to protect the organization from Spam and virus infected emails. Mail gateway relay server of such provider

	<b>POLICY</b>	Page #	6 of 8
		Revision number	7.0
	<b>INFORMATION SECURITY</b>	Effective Date	May 01, 2016
		Last reviewed on	December 22, 2022
		Next review date	December 21, 2024

will be used for email exchange with external world.

5.2.6. Email System Backup is being governed as mentioned in Data Backup SOP.

5.2.7. For ensuring Security of emails on handheld devices, Mobile Device Management software is deployed and security policies will be enforced through such software.

### 5.3. MOBILE DEVICE SECURITY:

5.3.1. Use of a Smartphone in connection with Atul business is a privilege granted to Managers through approval of their Business | Unit Head. User has to submit the email request on [admin@atul.co.in](mailto:admin@atul.co.in) along with business head approval.

5.3.2. IT manager will review the request and seek approval of IT head to provide access of corporate email on handheld device.

5.3.3. IT manager will intimate site engineer to configure user's handheld device and to load MDM software. Users who are on field will be guided through telephone for the required setup.

5.3.4. It is mandatory to have security PIN | Passcode or pattern on the device in order to protect against unauthorized access of device.


5.3.5. Account Password guidelines mentioned in Email account SOP will be applicable for the email client configured on the device.

5.3.6. Certain Input | Output ports such as USB, Camera, Bluetooth etc. may be blocked based on controls enforced through MDM software.

5.3.7. Prior to upgrading software of existing Mobile Device | upgrading personal Mobile Device, user is expected to consult IT Team.

5.3.8. In the event of loss or theft of a mobile device, the Manager should immediately report thefts to the IT Unit. In relation to theft or loss of a mobile phone, the user should also notify the Telephone Service provider directly.

5.3.9. In order to ensure integrity of company data and to ensure that it remains safe, your device will be remote wiped if: (i) you lose the device; (ii) you terminate employment with the company; (iii) IT detects a data or policy breach or virus

	<b>POLICY</b>	Page #	7 of 8
		Revision number	7.0
	<b>INFORMATION SECURITY</b>	Effective Date	May 01, 2016
		Last reviewed on	December 22, 2022
		Next review date	December 21, 2024

infection. In view of above it is essential that you ensure regular backup of your personal data in order to restore the same incase required. Company will not be responsible for any loss of personal data or application.

5.3.10. In addition to the above security precautions, all users are expected to use their device in an ethical manner.

5.3.11. Company reserves the right to revoke the privileges in the event that Managers do not abide by the policies and procedures.

#### 5.4. ENDPOINT SECURITY:

5.4.1. Blocking the use of USB mass storage | other removable storage and optical drives (CD|DVD writers)

5.4.1.1. Disable copying of data into USB mass storage devices by blocking USB ports of all desktops and laptops connected to the network of Company at Atul, Ankleshwar, Ahmedabad, Dadar, Goregaon and Thane.

5.4.1.2. Disable CD|DVD writer software on all desktops and laptops.

5.4.2. The controls will be achieved through the centralized endpoint security server located at Atul Datacenter.


5.4.3. It may be noted that there will be no restriction in the use of other USB devices such as mouse, keyboards, printers, etc.

#### 5.5. SECURITY MONITORING:

5.5.1. IT manager will monitor access of the internet using a log viewer and reports available on Firewall. Historical logs of internet access will also be reviewed in order to identify any policy violations.

5.5.2. IT manager will review content filter logs on every first Wednesday of the month.

5.5.3. IT manager will monitor server administrative activities through review of audit

	<b>POLICY</b>	Page #	8 of 8
		Revision number	7.0
	<b>INFORMATION SECURITY</b>	Effective Date	May 01, 2016
		Last reviewed on	December 22, 2022
		Next review date	December 21, 2024

logs of server and firewall admin activities using admin event logs.

- 5.5.4. IT manager will ensure that set SOPs are followed for account creation | revocation and monitoring of critical security infrastructure in order to avoid any policy violation.
- 5.5.5. In case a policy violation is observed, the concerned user | administrator is informed and will be asked to refrain from carrying out such activities. An email will be sent to the user with copy to his | her L+1.
- 5.5.6. Appropriate changes in Process | configuration will be carried out in order to avoid repetition of such incidence.

## 6. ABBREVIATIONS:

IT – Information Security

CISO – Chief Information Security Officer

## 7. VERSION HISTORY:

Revision no	Date	Description of Changes made
1.0	01/05/2016	New
2.0	01/03/2019	Reviewed and updated
3.0	19/01/2021	Reviewed and Policy format changed
4.0	20/07/2021	Clause added for firewall log retention
5.0	21/02/2022	Clause (5.4) added for Endpoint Security
6.0	19/09/2022	Modified "Authorized by"
7.0	22/12/2022	Modified "Authorized by"