Mindtree

Mindtree Limited

Information Security Policy

Version 2.3 | 11-Sep-2017

Copyright Information [1]

Revision History

Please keep the latest version on top

Ver	Change Description	Sections	Date	Author	Reviewer	Approver
2.3	Updated Internet Connection section and access control policy	13 and 14	11-Sep-2017	Satish Dorepalli	Subramanyam Putrevu	Ram C Mohan
2.2	Updated Network Connection section	15	22-Feb-2017	Satish Dorepalli	Subramanyam Putrevu	Ram C Mohan
2.1	Updated Compliance review	5	12-Aug-2016	Satish Dorepalli	Subramanyam Putrevu	Ram C Mohan
2.1	Updated Compliance review and access control policy	5	12-May-2016	Satish Dorepalli	Subramanyam Putrevu	Ram C Mohan

2.0	Updated Compliance review and access control policy	5 and 13	30-Jan-2016	Satish Dorepalli	Subramanyam Putrevu	Sushanth Pai
1.9	Incorporated changes to address findings from ISO 27K Gap Assessment – updated Information Security Policy Statement	Sec 4	2-Apr-2015	Satish Dorepalli	Subramanyam Putrevu	Sushanth Pai
1.8	Added security policy for application development	23, Application Security	4-Feb-2015	Satish Dorepalli	Subramanyam Putrevu	Venkatraman G S
1.7	Annual review prior to publishing on QWikMind		21-Jul-2014	Satish Dorepalli(Associate Director) - Corporate Information System)	Subramanyam Putrevu	Venkatraman G S
1.6	Yearly review and added the section on Threat management	All	06-Jan-14	Satish Dorepalli(Associate Director) - Corporate Information System)	Sudhir Kumar Reddy (CIO)	Shrish Kulkarni CISO)
1.5	Yearly review of the added policy, exception handling	All	28-Feb-13	Satish Dorepalli(Associate Director) - Corporate Information System)	Sudhir Kumar Reddy (CIO)	Shrish Kulkarni CISO)

1.4	Yearly review of the policy	All	19-Oct-11	Satish Dorepalli(Associate Director) - Corporate Information System)	Sudhir Kumar Reddy (CIO)	Shrish Kulkarni CISO)
1.3	Wireless Access Policy has been updated	19	14-Mar-11	Satish Dorepalli(Associate Director - Corporate Information System)	Sudhir Kumar Reddy (CIO)	Shrish Kulkarni CISO)
1.2	Reviewed all sections	All	21-Oct-10	Satish Dorepalli(Senior Manager - Corporate Information System)	Sudhir Kumar Reddy (CIO)	Shrish Kulkarni CISO)
1.1	Reviewed all sections	All	07-Apr-09	Ramesh Kumar T (Associate Director – Infrastructure Management)	Parthasarathy N S (CISO) Puneet Jetli (Senior Vice President & Head - People Function)	Parthasarathy N S (CISO)
1.0	No changes, Baseline Version	All	11-March-09	Ramesh Kumar T (Associate Director – Infrastructure Management) Sudhakara Thota (Associate Director – Administration)	Parthasarathy N S (CISO) Puneet Jetli (Senior Vice President & Head - People Function)	Parthasarathy N S (CISO)
0.5	Yearly revision of IS usage and security Policy	All	11-Aug-2007	Abhay Goyal Ramesh Kumar T Vikram Poovanna Arun Desai		Krishnakumar Natarajan (CEO)

References

Reader should read this document in conjunction with the following documents

No	Document Name	Ver	Location
1.			
2.			

Table of Contents

Purpose & Scope of this document

This document broadly outlines Mindtree's present Information Security Policy and applies to all users of Mindtree infrastructure facilities and recipient of Mindtree confidential Information and Information Asset(s).

This document is confidential to Mindtree and may be shared with Mindtree's Customers under appropriate agreements such as a NDA and / or MCA. Mindtree's Customers shall not share and / or publish this document.

Definitions, Abbreviation and Acronyms

The terms in use in the document are explained below

Acronym	Description
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
IS	Information System
ISMS	Information Security Management System
ISO27001	International Standard for Information Security Management
MCA	Master Consulting Agreement
NDA	Non Disclosure Agreement
ODC	Offshore Development Centre
PDA	Personal Digital Assistant
SEZ	Special Economic Zone
SLA	Service Level Agreement
STPI	Software Technology Parks of India
CIS	Corporate Information System
PII	Personally Identifiable Information
IT	Information Technology

Asset

Asset is something which has a definite value to the organization. There are various types of Assets in "Information Security Context" Viz., Physical Asset (Server, Generator), Information Asset (Source Code, Procedure Document, Design Document), People Asset (Project Managers, IS Manager, Security Guards, Admin Executive, Software Engineers), Service Asset (email, ISNet, Peoplehub, Internet), Software Asset (Binaries, installable, Builds, VM Images) and Paper Asset (Software License Agreements, Service Level Agreement, Employee Records, Contracts, Visitors Book)

Availability

Availability means ensuring that authorized users have access to Information Asset(s) and associated assets when required.

Business Partner

Business Partner means any organization, entity or individual who is neither a Supplier nor a Customer but shares and uses the Information Asset(s) by virtue of its business association with Mindtree. Entities such as banks, clearing houses etc would fall in this category.

Customer

Customer means any organization, entity or an individual who uses Mindtree services and includes prospective Customers who have expressed intent to use the services of Mindtree.

Confidentiality

Confidentiality means ensuring that Information Asset(s) is accessible only to those who are authorized to have access with the required approval and undertaking of confidentiality obligations, if needed.

Executive Management

Executive Management (also referred as Mindtree) means the Senior Management of the Mindtree comprising the Chairman and CEO of various groups/divisions.

Information Asset(s)

Information Asset(s) means any information relating to Mindtree business held in electronic and / or non electronic, printed or any other form.

Information System (IS) Infrastructure

IS Infrastructure is the Information System network of Mindtree managed by Mindtree IS team and its partners and consists of its Local Area Network and Wide Area Network and all connected components, e.g. routers, switches, servers, hosts, storage devices, PCs and printers etc.

Integrity

Integrity means safeguarding the accuracy and completeness of Information Asset(s) and processing methods.

Policy

Policy means a written statement of direction of the agreed best way to achieve the security goals relating to the Information Asset(s) of Mindtree. This policy maybe amended from time to time and it is the responsibility of each User to be aware of it.

Supplier

Supplier means any organization, entity or any individual who provides goods or services to the Mindtree and includes prospective Supplier who has bid for providing goods and services to Mindtree.

User

User means the person natural or juristic who has access to the Information Asset(s) of Mindtree who can either be a Mindtree Mind or a Customer or Supplier or Business Partner or any person associated with Mindtree in any capacity.

1 Introduction

Information is one of the key business assets of Mindtree and is essential to conduct its day to day business. Information is vital to achieve the overall business goals of Mindtree. The need to protect all Information Asset(s) is imperative as it not only contributes to the value and goodwill of Mindtree but is part of Mindtree's culture and philosophy of maintaining Confidentiality, Integrity and Availability.

2 Objective

To preserve the Confidentiality, Integrity and Availability of Information Asset(s), Mindtree has composed an Information Security Policy which defines:

- the point of view of the Executive Management on securing Mindtree's Information Asset(s)
- identification of Information Asset(s) and assigning ownership
- the rules for appropriate use of Information Asset(s)
- the management of Information Security
- the responsibilities of users in using and securing Information Asset(s)

3 Applicability

This policy applies to all users using Mindtree facility/infrastructure. In addition, Users working in ODC shall adhere to Customer Security Policy.

In absence of a Policy or a contradiction in usage terms for a specific situation, user should contact Mindtree CISO, who will liaise with the Customer to identify an appropriate resolution.

4 Policy Statement

"Mindtree is committed to managing and improving the security of all critical information assets through deployment of adequate protection measures and user training".

This Policy is endorsed by the Executive Management and shall be read, understood and complied with by all users who have any form of access to Information Asset(s). This Policy is the base from which further Information Security Policies may be created and implemented in accordance with ISO27001. The Information Security Policy shall be formulated to take into account business, legal, contractual & regulatory requirements.

5 Compliance and Review Policy

Compliance with this Information Security Policy is mandatory for all functions in the scope unless specific waivers are approved by CISO. This policy shall be revised and amended by the Security forum as and when changes are required.

Periodic internal and third party audits shall be initiated by the management to test the compliance to this policy, such audits have to be approved by CIO, IT Infrastructure head, Intranet application head or CISO. Any noncompliance identified during audits will be investigated and addressed. Process owners are responsible for ensuring that remedial measures are implemented appropriately within the stipulated period. Such third party audit include PCI-DSS compliance, SSAE-16 assessment at an organization level or particular vertical line of business.

Mindtree does not provide an access to entire corporate IT Infrastructure or ODC to any third party company using third party tools and scripts for any kind of technical assessment as it violates the commitment to our customers.

Mindtree follows Information Security handling guidelines while dealing with customer's sensitive data, the data may include PII. If mandated to follow customer mandated guidelines, Mindtree users would be informed accordingly.

6 Monitoring Policy

Mindtree reserves the right to monitor activities performed by users while they work within Mindtree facility or use Mindtree infrastructure. Mindtree does not provide an access entire network or systems to any third party company for any kind of technical assessment as it violates the commitment to our customers. Users who violate Mindtree policies shall be subjected to disciplinary action and other legal action, including but not limited to claims for damages and/or specific performance. Anomalies observed during such monitoring activities shall be reported as security incidents.

7 Personnel Security Policy

Mindtree is responsible to hire and retain people who possess the required credentials. Credential verification/screening will be conducted to verify previous employments of the person. Mindtree has a right to verify and retain copies of such records. Every user shall sign a confidentiality and non-disclosure agreement as part of their joining formalities. Mindtree shall provide all users necessary training and awareness on their security responsibilities. It is mandatory for every user to undergo the awareness training.

During termination of employment/contract, Mindtree shall take adequate care to recover all Mindtree assets from users.

Users who violate security policies of Mindtree shall be subjected to disciplinary action.

Contractors, are obliged to comply with the verification requirements as defined by Mindtree.

8 Acceptable use policy

Mindtree users have been provisioned with basic resources to perform their duties for business purpose, these resources include facilities, email, internet, laptop, desktop, software and other IT environment. By accepting terms and conditions during system login, the users accept to use these resources for business purpose only.

Limited usage of these resources is permitted within acceptable and reasonable period of time. Mindtree reserves to monitor the activities carried out using corporate resources, users misusing these resources shall be subjected to disciplinary action.

9 Physical Security Policy

Mindtree is responsible to provide a safe and secure facility for all users.

Perimeter Security shall be provided at every Mindtree location, as appropriate to protect the information processing facilities. Protection shall be provided through access controls so that only authorized personnel enter the facility. There shall be a clear demarcation between public access and secure areas.

Photography is strictly prohibited within identified secure areas of Mindtree. Sensitive areas of the facility shall be monitored by security surveillance cameras or patrolling.

Every user of Mindtree facility shall be provided access card and photo identity card. There will be differentiated identification for Mindtree Mind, contractor & visitor by the type of identity card issued and the lanyard coloring. All users shall wear their identity cards visibly while within the facility.

Visitor's entry into Mindtree premises shall be allowed only after due authorization by Mindtree Minds. Visitors shall be accompanied at all times by a user within Mindtree mind.

10 Equipment Security Policy

Mindtree facilities come under the STPI and/or SEZ regulations and have been identified as bonded warehouse units. All equipment movement is strictly controlled as a compliance requirement of these regulations. Records shall be maintained for all equipment movement between facilities and outside the facilities.

All equipment containing storage media and independent storage media devices shall be checked to ensure that sensitive data and licensed software have been removed or securely overwritten prior to transfer of ownership or disposal.

11 Laptop Security Policy

Mindtree/Customer issued laptops shall be clearly identified as company property. Users are responsible for the safety and security of their laptop.

Visitors carrying laptops into Mindtree facility is strictly discouraged. However, if justified based on business needs, it could be allowed, after registering the laptop identification details. The escort is responsible to ensure that the visitor laptop is not connected to Mindtree network. On authorization, visitors could be allowed to connect into a segregated network.

12 External Software Policy

All corporate desktops and laptops would be configured to be part of Mindtree domain. Any external device including laptop installed with any licensed or freeware tools would not be allowed to be plugged into corporate network. Mindtree reserves the right to refuse any software to be installed on its network unless CIS team deems it appropriate and secure.

13 Access Control Policy

Each user shall be provided a unique username & password to access Mindtree domain resources. Usage of strong password is mandated. User access assignment shall follow "least access" and "least privileges" policy based on their role in the organization. Any escalation of privileges or access shall be provided with an approval. Access to USB storage devices, any other portable storage ports/devices on user systems is restricted based on competency, exceptions are handled through approvals based on business justification. Users are responsible for any malicious acts perpetrated using their credentials. Users are responsible for backing up critical data onto designated storage area and indicate the data retention requirements. The hard disk drive on laptop is encrypted, the encryption key is tightly integrated with corporate active directory.

Data of people who have exited from Organization will be retained in central repository based on their competency and access to this data, would only be provided after a formal authorization approval email.

14 Internet Access Policy

Mindtree provides Internet access to users for business requirement. Access to internet is secured by implementing adequate firewall/filtering controls & routed through designated proxy/firewall. Access to additional internet resources shall be allowed on need basis with prior approvals. Internet access from corporate network is allowed only after valid domain authentication.

All systems and network usage shall be logged & monitored. None of the network devices are directly exposed to internet, they are all configured behind the firewall.

The devices exposed to internet undergo vulnerability assessment and penetration test at scheduled interval, the assessment is done by third party.

15 Network Connection Policy

Users shall not connect unauthorized devices in the production network. Segments of Network shall be segregated and secured as per business need.

16 Wireless Access

Mindtree has implemented secure wireless access into corporate network using active directory services authentication. Rogue wireless devices are detected using the administrative tools and appropriate action is initiated to disable such rogue devices.

This policy prohibits access to Mindtree networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Mindtree Security Team are approved for connectivity.

17 Business Continuity & Disaster Recovery Policy

Mindtree shall address business continuity at organization level, which would be addressed at content, site, city & state level. Project level business continuity plans shall be planned and implemented as per customer contracts, if any.

For identified natural and manmade disasters, emergency response and recovery plans shall be developed and implemented.

18 Mobile Computing policy

Mindtree shall allow mobile computing using laptops, PDAs, etc in order to enhance productivity. Such usage shall adhere to the necessary authorization and safeguards. Mindtree minds shall be provisioned remote access to work remotely with an authorization.

19 Change Management Policy

Any major changes made to infrastructure - physical or technology which may have considerable impact on the security posture of Mindtree shall be implemented only after seeking approval through formal change management process.

Every year Mindtree engages third party vendor to carry out vulnerability assessment and penetration test on Mindtree's internal and external network environment. This exercise is performed until desired results are achieved.

20 Vendor Management Policy

Confidentiality clause shall be added as part of all vendor contracts. Service Level Agreements (SLA) shall be established & monitored.

21 Security Incident Management Policy

Security incidents or weaknesses shall be reported by users through incident reporting procedure. A Root Cause Analysis shall be conducted by incident response team and necessary corrective/preventive actions shall be taken to remediate an incident

Depending on nature of incidents, customers are kept informed of actual or suspected breach through agreed mechanism of communication.

22 Information Security Awareness Policy

All new users are provided information security awareness training as part of the new hire orientation/assimilation program.

It is the responsibility of managers to ensure that team members undergo ongoing sessions on Information security and are kept updated on current information security policies, procedures & guidelines at least once in a year.

The Information Security Policies and Processes which users need to be aware shall be made available to authorized users over intranet portal.

23 Application Security

Mindtree application security standard for development, serves as a supplement to Mindtree's overall information security policies. Adherence to Mindtree application security standard will enhance the security of applications and help safeguard against standard security threats and vulnerabilities. Following are the key security practices to be adhered to during application development and deployment.

- Secure coding guidelines to be adhered to in order to safeguard against threats and vulnerabilities
- Ensure application errors do not inadvertently expose detailed system information
- Ensure applications logs are stored in a controlled environment
- IP protection through adequate policy guidelines
- Source code access control to be used in order to ensure it is accessed by authorized personnel
- Conduct application security testing using Mindtree standard framework as required

Mindtree Limited

Contact Information

Satish Dorepalli
Email: satish_dorepalli@Mindtree.com
Ramanujan IT City, TRIL
Rajiv Gandhi Salai, Taramani
Chennai – 600113
INDIA
Phone- 91 (44) 66711313
Fax- 91 (44) 66711001
Web- www.Mindtree.com