Information Security Policy

Version 1.2

Effective Date: 20-01-2019

Document Revision History					
Date	**Version**	**Description**	**Author**	**Reviewed by**	**Approved by**
01-Aug-2015	0.1	Draft-Information Security Policy-Crestech Software Systems Pvt Ltd	Vijay Khaware	TBR	TBA
08-Aug-2015	1.0	Baselined	Vijay Khaware	Lalit Jain	Lalit Jain
29-Jan-2017	1.1	Baselined	Vijay Khaware	Lalit Jain	Lalit Jain
20-Jan-2019	1.2	Baselined	Vijay Khaware	Lalit Jain	Lalit Jain

Contents

Information Security Policy

1 Purpose

This Policy will provide the means of protecting Crestech's information and information systems from unauthorized access, use, or disclosure to the unauthorized personnel. This policy will also help in achieving the 3 major goals i.e. confidentiality, integrity and availability of Crestech's information.

2 Scope

The scope of this policy will imply to the following:

- All Crestech's Employees;
- All personnel having some sort of Contract (service providers) with Crestech and have access on various resources like information or systems;
- Former employees of the company that may have access to the systems or any information.

Definition of Resources:
It means servers, systems, laptops or internet access that is given to employees or contractors or former employees to conduct their official responsibilities.

3 Policy

Confidentiality means protecting disclosure of the information to unauthorized individuals or systems irrespective of that individual being a Crestech's Employee or not.

- Employee shouldn't be disclosing any confidential information to any unauthorized personnel.
- Employee shouldn't be using the information or systems for its own use or betterment.
- Employee shouldn't be discussing any information with clients that are supposed to be kept confidential within the organization.
- Employee shouldn't be disclosing anything that are marked or rated as confidential at the time of termination either from the organization or from the current engagement.
- Employee should treat all information as confidential (by default), in case there is a no clarity on the information.
- Employee shouldn't post any information on public web sites or blogs. Hence making acceptable use of Internet Resources.

- Employee must adopt a clean desktop policy i.e. no papers or documents should be left unattended when an employee is not near to the workstation.
- Documents or diary or any related stuff should be marked as “Confidential” so that others couldn’t touch them.
- Employee shouldn’t leave the workstations unattended. Workstations must either be in logged off or locked down state.
- Sensitive documents should be disposed of using shredders.
- Access on data or any information should be given to the individual (s) having business justification.
- All Crestech’s system should invoke a password protected screen saver, if the systems are left unattended for more than 10 minutes.
- Data inside the personal storage system (like mobile, PDA, USB Drives) should be kept with extreme caution and it shouldn’t be disclosed to any unauthorized personnel.
- Data transmitted using any means to the client should have a business justification or need.
- No sensitive information should be sent over an Instant Messaging Application.
- Crestech’s Employee shouldn’t be forwarding any information using emails or internet or by any other means if the recipient is not the one who should be receiving it. and Password
- Sharing Domain Credentials under any condition is treated as an offence in Crestech. No employee under any circumstances should share the domain credential, which may breach the data security and confidentiality agreement.
- Employee should change the password once in every 30 days.
- Crestech may monitor each and every activity that a user may perform on the system starting with sending or receiving emails up to accessing web sites visited, any stuff downloaded from or uploaded to the Internet.
- Crestech may use from monitoring software to check the validity and integrity of the data being sent and received by the employees using various communications means like emails, internet etc.

Available Resources that Crestech provides to its employees are workstations, access to Internet and emails etc, which should solely be use for business related purpose.

- Employee shouldn’t indulge in any illegal activities using company resources.
- Employee shouldn’t disclose any company related information with unauthorized personnel.
- Employee shouldn’t use the company resources for extensive personal use. However, a minor usage is allowed.
- Employee shouldn’t company resources to have business relations with any other company or competitor

- Employee shouldn't click on URL sent via Messenger during any conversation, which could impose a security threat to an environment.

- Employee shouldn't use any software unless it is authorized by the IT department, exclusively signed off by the management.

4 Implications

Crestech strictly follows the information security policy as designed and defined above. Crestech management works with their HR and IT department to conduct a surprise Audit to verify if all employees are rigorously following the defined approach.
Crestech has all the rights reserved to take any sort of disciplinary action against the one not following this policy.