

Vision - To build a secure and resilient cyberspace for users and businesses.

Objectives - To create a secure cyber ecosystem in the organization, generate adequate trust & confidence in IT systems.

To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem in business application and enhance the protection and resilience of DC and DR critical infrastructure.

Strategy -

1. Rules for using email encryption - we are using O365 that has been point to point encrypted in cloud of Microsoft India.
2. Steps for accessing work applications remotely - Our business application SAP Hana 1809 is configured thru router string with 24x7 remote accessing availability, without web based services.
3. Guidelines for creating and safeguarding passwords - as per password policy.
4. Rules on use of social media - as per internet policy defined in firewall.

Virus Protection policy - Antivirus is in place with the following protection:

- ❖ It helps to detect, removes, and repairs the side effects of viruses and security risks.
- ❖ It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- ❖ It helps to detect the applications that exhibit suspicious behaviour.

Firewall Policy - Policy activated and provides the following protection:

- ❖ Blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- ❖ It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.