Information Security Policy

SOP TITLE	Information Security Policy
SOP NUMBER	IT.001
STATUS	Approved
VERSION NUMBER	1.0
EFFECTIVE DATE	November 01, 2022
REVIEW DATE	November 01, 2022
NEXT REVIEW DATE	November 01, 2023
BUSINESS | UNIT	IT
DEPARTMENT | FUNCTION	IT Infrastructure
INITIATED BY	Dibyojyoti Roy – Sr. Manager - IT
REVIEWED BY	Subir Hore – General Manager - IT
APPROVED BY	Partha Protim Mondal – Vice President & Head IT
ANNEXURE LIST	None

Purpose

Information is an integral part of the organization. Such information is accessible by the employees of the organization through various IT resources which include computing, networking, applications, and telecommunications. The Information Security Policy of the organization defines rules, regulations and guidelines for the ethical usage of such information to protect business data in a secured manner and prevents from any cyber threats.

Ownership

Head Office - IT

Responsibility

All users of the organisation.

Policy Statement

Guidelines to ensure information security data protection of the endpoints (desktop, laptop, servers) and prevention from any external threats.

Endpoint Security

1. The endpoint agent is implemented in identified business critical desktops, laptops, and all servers of our DC (data centres).
2. The agent installed for the first time executes full scan of the endpoint and captures the data for necessary threat analysis. From next time onwards, it scans the incremental change only.
3. If any file is found to be infected by any malicious threats, it is either quarantined or cleaned or deleted based on the severity of the threat. It prompts proper message to the user for information and captured in the log file for future analysis.
4. Threat alerts of respective endpoint is captured in the dashboard for Threat analysis.
5. MDR (Managed Detection and Response) team from product group (CrowdStrike and Sentinel One) monitors the end-point logs on 24 X 7 basis for necessary threat analysis & hunting and invokes necessary actions to maintain secured environment.
6. The endpoint application is updated on a periodic manner as configured by the product group and user is responsible to allow the upgrade process.
7. It is the responsibility of each user to ensure that endpoint security agent software is updated on a regular basis.
8. In case of external storage device like pen drive, hard disk or CDROM / DVDROM on connection to the endpoint, the endpoint software is configured to scan automatically all the files. However, it is a good practise to scan manually external device(s).
9. If any aberrations are experienced, the user should approach the concerned IT person without any delay and fix up earliest possible time for resolution.

FPR (First Person Responsible) Matrix:

Level	FPR	Email ID	Contact Number
1	Ashim Debnath	ashimdebnath@bergerindia.com	9147161524
2	Dibyojyoti Roy	dibyojyotiroy@bergerindia.com	9230018095
3	Subir Hore	subirhore@bergerindia.com	9230017702

User Access Management

1. All users are provided with domain login id to access their respective endpoint (desktop/laptop).
2. Only active domain login id will provide access to a set of applications such as Mail, SharePoint, Antivirus, and organisation's network.
3. Active domain login id is a mandatory intermediate step to access other business applications using application specific username / password such as Oracle ERP, MS CRM, Supply Chain Planning–o9, Darwin Box, etc.
4. No user can install / uninstall any application on their endpoint. No one is authorised to download any software from internet, even if anyone downloads any software the domain login id will be blocked and will be penalised appropriately. Also, the endpoint will not allow to install the downloaded software.
5. All users have the privilege to send/receive mails using organisation provided mail system.
6. All business user does not have access to any of the application servers, network devices and databases.
7. Whenever the user connects to Berger network in office or remote site, the system health of the device is verified by the System Centre Configuration Management (SCCM) for latest patches of windows and anti-virus. If the existing version of endpoint is equal or higher then it allows user to get connected with organisation's network otherwise disallowed.
8. As part of an employee joining process, HR provides the detailed information about the employee including the roles & responsibilities assigned along with the requisite access to applications.
9. Except authorised IT employee, no one is allowed to access restricted areas like server, network, UPS, etc.
10. Authorised IT employee is allowed to access the restricted area (data centre) using separate access cards or finger screening.
11. Remote Access
    a) Organisation allows approved users to access Berger applications from offsite locations over the internet by using Virtual Private Network (VPN) technology.
    b) Policy governs controlled application access and safeguards misuse of company information by restricting unauthorised access to Berger network & application.
    c) Remote access to business application will only be allowed after successful identification and authentication of the users.
    d) The remote access is allowed only through secured communication channels as defined in Microsoft Direct Access (DA) and VPN (Cisco or Fortinet).
    e) Application access to the users depends on the given roles & responsibilities.

Password Management

1. Active directory service prompts the user to change the password for every 45 days, otherwise the user account gets locked.
2. System will prompt to change the password for the first login.
3. Active directory validates the password combination as configured in the system as per company password policy.
4. Password complexity
    a) Password is case-sensitive.
    b) Password is minimum 8 characters and maximum 20 characters.
    c) Password has to be a combination of alphabets (a,b,c,d.....z, A,B,C,D .....Z) numeric (0,1,2,3....9) and at least one special character from (!#$%&'()*+,-./:;<=>?@[\]^_{|}~).
5. Ethical practise in assigning new password
    a) Refrain from using the previous password as new password.
    b) Do not use the default password "berger@123" or similar passwords like "berger@1234", as these passwords are very much susceptible to cyber-attacks.
    c) Do not use your username / user id / login id as part of the password.
    d) Create long, unique, and hard to guess passwords. Never keep the same password for different online accounts.
    e) Change your Internet banking passwords at periodical intervals and never share them with anyone.
    f) Keep passwords that have a mix of uppercase and lowercase letters, numbers, special characters, and are at least 8 characters long.
6. Recommended Password Settings

Minimum Password Length	8 characters
Maximum Password Length	20 characters
Password Age	45 days
Prompt user to change password before expiration	13 days
Password history	1 password remembered
Password complexity	Enabled
Never expiry of password	Disabled for users

7. Recommended Account Lockout

Account Lockout	Enabled
Lockout after	5 attempts
Lockout duration	Until administrator unlocks

8. Password Change Process
    a) It is recommended to change system password frequently.
    b) The system forces to change the password after 45 days.

c) If the user is connected in in office LAN, Press CTRL+ALT+DEL key from keyboard and select "Change Password" option.
d) If the user is on internet, open the URL https://bpilexchange.bergerindia.com/owa/auth/expiredpassword.aspx, type in the User Id/Login ID as the Username and change the password.

9. Password Reset Process: Users may forget their password or password gets expired, in such case the same has to be reset by Mail Administrator only on the basis of mail request (can use personal or colleagues mail id) through his/her reporting manager or HR.
10. Privileged Password Maintenance
    a) "Never Expiry of Password" option is enabled for super user or administrator of the servers.
    b) Such password is allocated to only limited and identified users only. All such requests are addressed to and approved by IT Unit Head.
    c) All critical passwords are being saved in excel format and encrypted on central server and shared with only identified users.
    d) The password for highly privileged users e.g. superuser or administrator will be stored in a sealed envelope and placed in a secured location under the custody of IT Unit Head for emergency usage.

11. her business applications using application specific userid / password such as Oracle ERP, MS CRM, Supply Chain Planning–o9, Darwin Box, etc.
12. No user can install / uninstall any application on their endpoint. No one is authorised to download any software from internet, even if anyone downloads any software the domain login id will be blocked and will be penalised appropriately. Also, the endpoint will not allow to install the downloaded software.
13. All users have the privilege to send/receive mails using organisation provided mail system.
14. All business user does not have access to any of the application servers, network devices and databases.
15. Whenever the user connects to Berger network in office or remote site, the system health of the device is verified by the System Centre Configuration Management (SCCM) for latest patches of windows and anti-virus. If the existing version of endpoint is equal or higher then it allows user to get connected with organisation's network otherwise disallowed.
16. As part of an employee joining process, HR provides the detailed information about the employee including the roles & responsibilities assigned along with the requisite access to applications.
17. Except authorised IT employee, no one is allowed to access restricted areas like server, network, UPS, etc.
18. Authorised IT employee is allowed to access the restricted area (data centre) using separate access cards or finger screening.
19. Remote Access
    f) Organisation allows approved users to access Berger applications from offsite locations over the internet by using Virtual Private Network (VPN) technology.

g) Policy governs controlled application access and safeguards misuse of company information by restricting unauthorised access to Berger network & application.
h) Remote access to business application will only be allowed after successful identification and authentication of the users.
i) The remote access is allowed only through secured communication channels as defined in Microsoft Direct Access (DA) and VPN (Cisco or Fortinet).
j) Application access to the users depends on the given roles & responsibilities.

Internet Usage

- **Basic Access**

1. The Internet access is provided to employee based only on business requirements.
2. User provided with the Internet facility has only http / https services available. Services like telnet, FTP requires approval from the Information Security Team.

- **Internet Connections**

1. All internet connections passed through a firewall and/or a proxy server.
2. Dial up internet access from the Office Network is strictly prohibited.

- **Approved Use**

1. Internet usage in the office premises or through office assets is not allowed for any unauthorised/unethical activities.
2. Unauthorized use of Internet includes, but is not limited to:
    i. Using for personal entertainment, personal business, or profit, and publishing personal opinions.
    ii. Soliciting money, personal gain, or in an illegal manner.
    iii. Attempting to gain or gaining unauthorized access to any computer system of Company or any other organization.
    iv. Sending racial, sexually threatening, defamatory or harassing messages.
    v. Sending, transmitting, or distributing proprietary information, data or other confidential Company information.
    vi. Performing deliberate acts (non-business-related use) that waste computer resources like uploading and downloading large files, accessing streamline audio and/or video files, playing games on the Internet and engaging in online chat groups.
    vii. Introducing computer viruses, worms, or Trojan horses.

viii. Downloading obscene written material or pornography.

3. Access to the Internet from a Company owned laptop or through Company owned connections adheres to the same policies as those within Company facilities.

- **Downloading of Software**

1. Software needed for business purposes, can only be installed by System Department, provided:
   i. The software has been verified by System Department / Asset Management / Legal.
   ii. The software has been scanned for viruses using the latest virus definition files.
   iii. The conditions or prerequisites for the usage of the software have been met.
2. Only System Administrator can install the specified software after adhering to the licensing norms and obtaining proper approvals.
3. Trial version of any software in use will be deleted after the trial period or will be procured to comply with the licensing norms.
4. The Asset Management Team periodically reviews workstations to verify that only approved and licensed software has been installed and running.
5. The Asset management Team provides the report of the review to the designated Manager and/or GM IT.
6. Organisation is not responsible for usage of any non-licensed and/or unauthorised software by employee and such offence, if found guilty, by audit team, can attract punishment.

- **Website Blocking**

1. Web content filtering proxy shall be installed to restrict the users from accessing content deemed inappropriate.

- **Dos and Don'ts of Internet Use**

1. While uploading any personal or financial information on any website, check if it's URL begins with 'https'. Also look for the lock icon, which indicates that the connection is secured.
2. Keep your computer's Firewall ON
3. Use your primary email address to stay in touch with people you know or are acquainted with.
4. Avoid using your official email address for social media sites.

5. While you are online in a public setting such as a coffee shop, mall, airport, etc., watch your back to make sure no one's snooping on you.
6. Never trust emails asking for your personal or banking information. Be extra cautions against links or attachments in unknown or unwanted emails. Verify any such communication with the sender first.
7. Do away with old accounts that you do not use anymore.
8. Never respond to pop up ads that may come up on your screen. Close such pop ups.
9. Downloading of any free software should have proper approval from Corporate IT team.
10. Avoid visiting inappropriate websites or websites that you are not fully aware of.
11. Beware of files with multiple extensions.
12. Always log out of online accounts when you are done.
13. Access your bank's website by manually typing its URL in the address bar.
14. Do not click any links in emails to access your bank's website.
15. Keep your software and operating system up-to-date.
16. Do not install software that comes as an attachment in emails.
17. Update the Internet browsers and software on your computer.
18. Use up-to-date security software that offers multilayered protection.
19. Increase your awareness of cyber security and share the same with friends and family.
20. Avoid saving your credit/debit card information on websites and web browsers.
21. Never share your financial details on phone or email, even if the caller/sender seems genuine. Remember, people in cyberspace are not always what they seem to be.
22. Avoid downloading software from unverified publishers.
23. Always lock your computer when not in use. Do not leave it unattended, especially in public places.
24. Protect your device with a screen lock. Turn the automatic screen lock function ON.
25. Install apps only from trusted and official sources.
26. Turn OFF Wi-Fi, Location Services and Bluetooth when not in use.
27. Avoid sending or saving personal & overly sensitive information on your mobile device.
28. Avoid mobile apps that ask for unnecessary permissions.

Firewall

1. Maintain three-layer architecture categorised as – Militarized Zone (MZ), De-Militarized Zone (DMZ) and Management Control Zone (MC).

2. Different firewall products are used in MZ and DMZ zone, so that both are not compromised at the same time.

3. Firewalls are configured with the following minimal mandatory rule sets:
   a) Block incoming packets having Internal IP address range.
   b) Block Private IP addresses segments reaching through internet.
   c) Allow restricted services between Internal Network & De-Militarized Zones (DMZs).
   d) Denies all services by default and allows required services only

4. Firewalls are configured for anti-spoofing.

5. Firewalls log files type such as; failure/deny are being reviewed on a regular basis (quarterly).

6. Administrative and User access to firewalls are only provided on a need basis to designated authorised user as per roles.

7. Encryption technologies are being used for Remote Administration on firewalls.

8. Access through firewalls are being granted on at least getting the below details and after due approval by security manager
   a) Source Address
   b) Protocol information
   c) Source port
   d) Destination port
   e) Destination address

9. Operating systems hosting firewall components are being tightened to the highest level of security, as per applicable OS hardening procedures.

10. Third party software are not installed on firewalls.

11. Internet usage procedure is being followed for hosting any internal server on DMZ/Internet zones.

12. Following activities are disallowed:

    a) IP directed broadcasts
    b) Incoming packets at the Firewall sourced with invalid addresses

c) TCP small services
d) UDP small services
e) All source routing
f) All web services running on Firewall
g) Use corporate standard SNMP community strings
h) Access rules are added as per organisation needs

13. Adequate care is being taken while changing the configurations of the firewall to ensure minimal distortion of the production environment.

14. Network based Intrusion Prevention System (IPS) is being implemented in the perimeter firewall where internet connection is terminated.

15. Any change in firewalls is being carried out by using TACACS+ (Terminal Access Controller Access-Control System Plus) which captures the audit trail having information like user, date-time stamp. TACACS+ also facilitates the services towards Authentication, Authorization and Accounting.

Abhijit Roy

- End of Document -