Document name	IT & Security Policy
Version no.	3.0
Release date	18-Aug-15
Abbreviated Name	ITSP_IS
Classification	Internal

IT & Security Policy

Document History

Ver. No	Release Date	Created By / Modified By and Date	Reviewed By and Date	Approved By and Date	Remarks and Changes Made
3.0		Snehal Jadhav 16-Dec-14			Transition of ISMS from ISO27001:2005 to ISO27001:2013 and made changes in section 12 User Accounts and Password in point l. procedure to unlock the user account as suggested by client.
3.0	18-Aug-15		Shailendra Kumbhar 17-Aug-15	Viraj Padhye 18-Aug-15	Approved.

Table of Contents

1. Introduction

For the purposes of this policy, Cybage Software Private Limited shall be referred to as “Cybage / Company / Us” and the employees of Cybage shall be referred to as “Employees / User / You”. “Client / Customer” refers to a Cybage client.

Information is integral to all of us and is the most important asset of the company. We are all exposed to Information on a daily basis while performing our jobs. Information is continuously modified or transmitted with the increased use of information assets like computer systems, email, internet and intranet. If such information is not handled properly then it may critically expose the company and its customers to incidents of data and intellectual property leakage eventually resulting in loss of revenue and reputation.

Cybage is committed to ensuring the confidentiality, integrity and availability of its data and computer systems. Cybage understands that security of information is an essential keystone of its operations. Each of us is continuously required to be focused on how we can securely handle the information. Vigilance, awareness and good security practices are the most valuable means we have of providing this protection.

2. Purpose

The purpose of this policy is to define an organization-level policy for all the IT services or facilities that are provided by Cybage to its employees. Clear understanding of this policy will assist you in your routine work and help defend you from circumstances that could put you and the company at any kind of risk.

3. Scope

This policy is applicable to all employees of Cybage. References to the grades of employees are made throughout the policy. Refer to the organization structure in the HR section on the Cybintranet to understand the same.

4. Mailing

4.1 Acceptable Usage

a. Company-provided email account or accounts must be used for official communications only. It must not be used for any personal communication such as, but not limited to, greetings, subscriptions, mailing lists, jokes, and graphic images. **[Severity: Low]**

b. Company provided email account or accounts must not contain offensive or disruptive messages, offensive comments about race, gender, age, sexual orientation, religion, political beliefs, national origin or disability **[Severity: medium]**
c. Users who are eligible to receive mail on handheld devices should manually move their mail to the pst located on their desktop/ laptops. For other users, IS dept. configures the mail client to download mails to the pst file on their desktop/ laptop. **[Severity: NA]**
d. Employees at level 3 and above designations and employees who are onsite are eligible for access to Cybage webmail. This access will be provided on request. **. [Severity: NA]**
e. Users with company issued laptops and with Microsoft Outlook client can send and receive mail using a feature called 'Outlook Anywhere' which will be configured by the IS Dept. on demand only. **[Severity: NA]**
f. Only Cybage email account and wherever applicable, the email account provided by the customer will be configured on your system. Other email accounts must not be configured on your system. **[Severity: Medium]**
g. The Cybage mail ID and the Cybage mail servers must not be used for testing activity. Employees must request a test mail ID for such purposes via the helpdesk. The IS department will issue a mail ID created in a test domain. **[Severity: medium]**
h. Users should not open URL's that appear in emails or email attachments from unknown sources. **[Severity: Medium]**
i. Anti-spam service is activated on all mailboxes. In spite of this, if the user receives more than 5 spam mails in a day, the user should log a ticket in helpdesk. Less than 5 mails are considered as acceptable. **[Severity: NA]**
j. If a legitimate mail is quarantined by the anti-spam service, users may retrieve it using the link **https://admin.protection.outlook.com/quarantine**. Alternatively users may visit this link once in a week to check for any mails that are quarantined. Quarantined mails are stored on the server for a period of 15 days only. Users may refer to the Microsoft Exchange Online Protection (EOP) Guide stored on the Intranet under IS >> News and Announcements for more information.**[Severity: NA]**
k. Users should trust only those mails from the IS Dept. that are digitally signed. Any mail from the IS Dept. that is not digitally signed should be reported to **sec_admin@cybage.com. [Severity: NA]**
l. Following quotas and mail attachment limits have been implemented for all users as per the designation

Quota and Limits				
Grade	Mailbox quota	Warning mail	Outgoing mail size allowed (incl. attachments)	Incoming mail size allowed (incl. attachments)
Management	2 GB	1.9 GB	-	-
DM/DH and higher grades	1 GB	900 MB	10 MB	20 MB
Managers and equivalent grades	100 MB	90 MB	7 MB	20 MB

All others	12 MB	10 MB	2 MB	20 MB

m. If required during travelling or before going on leave, employees at Level 3 and above may request their mailbox limit to be set to unlimited, which will be reverted to its original size within 2 days of the user returning to the Cybage office. For employees with designations other than the ones mentioned above, the mailbox quota will not be set to unlimited and they are required to download their mail to their laptops even while travelling. **[Severity: NA]**

n. Mail quota for users going on leave will be handled on a case to case basis. **[Severity: NA]**

o. Cybage FTP server should be used if attachments more than the size mentioned in the table above need to be transferred. **[Severity: Low]**

p. Mail for Exchange services on handheld devices is permitted only for employees at level 3 or higher. **[Severity: NA]**

5. FTP Server

Cybage uses Secure FTP server which provides a secure channel for data transfer. This ftp server is used by Cybage employees and its customers and hence the points mentioned below should be informed to the customers as well, if applicable.

5.2 Acceptable Usage

a. Cybage FTP server must only be used for official purpose. [Severity: Medium]

b. Only employees at Level 3 and above designations are eligible for an FTP account. [Severity: Medium]

c. Username for FTP server is generated separately by the IS Team upon request. The Windows user account cannot be used with the Cybage FTP server. Project Manager should request a separate user account for each user or client who requires access to the FTP server. [Severity: low]

d. Cybage FTP server works only in secure mode. Thus users need to use a FTP client with secure FTP support. [Severity: NA]

e. Cybage FTP server makes it mandatory for a user to have a strong password. Strong passwords are passwords that contain alphanumeric & special characters and do not contain three or more characters in series from the username.[Severity: NA]

f. Password expires every 45 days. Users will receive an e-mail notification to change the password 5 days before the date of password expiry, with subsequent notices every day for the next 4 days. Users will not receive any warning or notification mails after password has expired and will be required to log a helpdesk request. [Severity: NA]

g. Cybage has standardized Putty as the SSH client which should be used to change the password. [Severity: NA]

h. Cybage FTP server should not be used as a repository. Files older than15 days will be automatically deleted using a script without any prior intimation. [Severity: NA]

i. FTP folder for a project is created as per the abbreviated name of the project under MIS. The project manager decides who is given access to this folder along with the level of access. [Severity: NA]

j. Only 1 GB of disk space is assigned to each project. [Severity: NA]
k. In case of 3 failed login attempts, the IP address of the user would be automatically blocked and the user would not be able to connect to the FTP server. In such cases, the user has to request the IS dept. to get the IP unblocked. [Severity: NA]

6. Internet

Company provided Internet access should be used for business purpose only. Websites not required for work are either available under a quota of 60 minutes or blocked depending upon the nature of the website and its impact on the business environment.

6.1 Acceptable usage

a. Internet browsing is controlled using an enterprise internet filtering software. The table below lists the categories that have been permitted and ones that have been blocked. [Severity: NA]

Websense Policy - Default		
Always open	**Quota**	**Always blocked**
User-Defined	Entertainment	Adult Material
Financial Data and Services	News and Media	General Email
Information Technology	Traditional Religions	Bandwidth
Organizational Email	Shopping - Internet Auctions and Real Estate	Internet Radio and TV
Business and Economy	Social Organizations	Internet Telephony
Hosted Business Applications	Society and Lifestyles	Peer-to-Peer File Sharing
Education	Hobbies	Personal Network Storage and Backup
Government	Restaurants and Dining	Streaming Media
Health	Social Networking	Drugs
Search Engines and Portal	Sports	MP3 and Audio Download Services
URL Translation Sites	Vehicles	Gambling
Web Collaboration		Games
Web Hosting		Illegal or Questionable
Windows Updates (Custom)		Computer Security
Images (Media)		Hacking

Image Servers		Proxy Avoidance
Advocacy Groups		Web and Email Spam
Travel		Text and Media Messaging
		Web Chat
		Job Search
		Militancy and Extremist
		File Download Servers
		Productivity
		Freeware and Software Download
		Instant Messaging
		Message Boards and Forums
		Non-Traditional Religions and Occult and Folklore
		Security
		Blogs and Personal Sites
		Social Networking
		Special Events
		Violence
		Weapons
		Internet Communication
		Online Brokerage and Trading
		Professional Networking

b. The quota mentioned in the table above is of 60 minutes per day and is split into 6 session of 10 minute each. Users will get a page in their browser that informs them that the site can be viewed under quota after which the users may choose to start the 10 minute session. Once this session expires, the users will again get a web page that informs them that the session has expired and that the user can start another 10 minute session. [Severity: NA]

c. A few exceptions to the above default policy are made for employees at Level 3 and above. Categories like personal mail, professional networking, instant messaging and message boards and forums are allowed for these employees upon approval. [Severity: NA]

d. Remote Websense agent will be installed on all laptops to control internet access while working out of office. Potentially malicious websites will be blocked under this profile. [Severity: NA]

e. Websites that come under the categories that are “Always blocked” may, at times, be accessible due to server maintenance or other technical issues. Browsing these websites under such circumstances would still be considered a policy violation. [Severity: Low]
f. Instant Messengers are allowed only if it is a project requirement for official chat purpose. Multi-messengers are not allowed [Severity: Low]
g. Users must not bypass the internet restrictions imposed by Cybage. [Severity: Medium]
h. Only active mode is supported for connecting to any external FTP server. Users should set the web browsers and FTP clients to work in active mode to avoid connectivity problems.[Severity: NA]
i. All uploads should be related to the project or for official purpose only. Permission from IS team is required for uploading any large files on the internet. . [Severity: Medium]
j. All downloads should be requested by logging a helpdesk ticket. IS team may download this on your behalf or inform you when the download may be started.[Severity: Medium]
k. Employees should not start any bandwidth intensive activity like server synchronization, database downloads, etc. In working hours without taking prior approval from the IS Dept. [Severity: Medium]
l. A few projects are required to execute scripts that query search engines on the internet as part of their project activities. Employees should take approval from the Information Security team before starting such activities. [Severity: Low]
m. Email communication from the Cybage account and to personal webmail accounts like Gmail, Yahoo, Hotmail etc. is blocked.[Severity: NA]
n. Kiosks are provided for unrestricted internet access and users should understand that this environment is not secure. Thus it is not connected to the company network and no such access will be provided under any circumstances. The policy for the Internet kiosk is given below. [Severity: NA]

Websense Policy - Internet Kiosk		
Always open		**Always blocked**
User-Defined	Government	Adult Material
Bandwidth	Health	Computer Security
Internet Radio and TV	Illegal or Questionable	Hacking
Internet Telephony	Information Technology	Proxy Avoidance
Peer-to-Peer File Sharing	Web and Email Spam	Security
Personal Network Storage and Backup	Internet Communication	
Streaming Media	General Email	
Business and Economy	Organizational Email	
Financial Data and Services	Text and Media Messaging	

Hosted Business Applications	Web Chat	
Professional Networking (Custom)	Job Search	
Drugs	Militancy and Extremist	
Education	News and Media	
Entertainment	Productivity	
Gambling	Freeware and Software Download	
Games	Instant Messaging	
Social Networking	Message Boards and Forums	
Special Events	Online Brokerage and Trading	
Sports	Shopping	
Travel	Social Organizations	
Vehicles	Society and Lifestyles	
Violence	Blogs and Personal Sites	
Weapons		

6.2 Internet Bandwidth

This section defines the clauses related to internet bandwidth requirements of the projects within the organization.

a. The lead time for upgrading the bandwidth or procuring a new connection will take at least a month from the date of purchase order. However, this time may vary due to dependency on the 3rd party service provider. [Severity: NA]

b. Bandwidth usage reports can be provided to Cybage's clients, if required, for facilitating the billing. [Severity: NA]

6.3 Blogging

a. Employees should not post, on any website, any Cybage or customer proprietary confidential information (directly or indirectly) such as but not limited to references like email addresses, logo, trademark information, employee numbers, account information, internal project/customer information, financial information, strategic decisions, internal email excerpts, internal security details, Cybage as a name along with blog site domain name/blog site URL itself or any copyrighted material which are available to users by virtue of working with Cybage.[Severity: High]

b. If user has reasonable doubt on the sensitivity of information that would be posted, user should seek a written consent from their managers and Cybage legal team (legal_team@cybage.com) prior to such posting[Severity: High]

c. Blogging sites should not be used as a medium for carrying out any transactions/promotional activities on behalf / in the name of Cybage to any external parties by the user. [Severity: Low]

7. Backup

Data backup is necessary to prevent its loss in the event of equipment failure, data destruction (intentional/unintentional), or a disaster.

a. Information Systems department is responsible for taking backup of central servers like code repositories, database servers etc. Project Managers are expected to identify critical servers within their project and request the IS department to include them in the backup cycle. [Severity: NA]

b. If the PM fails to identify the servers and the server crashes, the project will have to pay the cost of data recovery. [Severity: NA]

c. All static data on project servers should be excluded from the daily backup. PM should raise a helpdesk ticket for the data that needs to be archived. [Severity: NA]

d. Audio and video files are excluded the backup data. . [Severity: Low]

e. Restoration drills are carried out quarterly for projects selected by the IS dept. on a random basis. A Project Manager may request his project to be included in this restoration drill by raising a ticket in helpdesk. . [Severity: NA]

f. If for any reasons the server cannot be backed up by the backup client, a folder will be provided on the backup server. It's the responsibility of the project manager to ensure that the required data is copied to this folder. [Severity: NA]

g. Only employees at level 3 and above are eligible for a backup client on their desktops/ laptops. [Severity: NA]

h. Employees at Level 3 and Level 4 are allocated 5GB of space for backup. Employees at level 5 and above are allocated 10 GB of space. [Severity: NA]

i. Employees at level 1 and 2 should not store business critical data on their desktops. Such data if lost under any circumstances will not be recovered. [Severity: NA]

j. Only business critical data should be backed up. Personal data should be excluded from the backup cycle. Personal data is defined as but not limited to salary slips, personal statements, images like personal photographs, audio/video files. [Severity: Low]

k. Static data on desktop/ laptop should not be added to the backup cycle, it should be archived instead. This is necessary to decrease the size of the data being backed up, reduce the backup and the restoration time and decrease network utilization. In some cases it may utilize the space quota allocated to the user and cause the backup job to fail. [Severity: Low]

l. Periodicity of backup (backup schedule) should be determined by the information owner. [Severity: Low]

m. Backed-up data should be verified for its integrity and effectiveness by restoring the data. [Severity: Low]

8. Network

Each project or department is limited to a logically segregated network called VLANs.

8.1 Acceptable Usage:

a. Connectivity between project VLANs is disabled by default. Due to this, the users in one project will not be able to access the machines in any other project. [Severity: NA]
b. Users should not change any settings related to the network such as IP address, DNS server, and DHCP settings configured on any host. [Severity: Low]
c. Users should not configure / install any network services such as DNS server, DHCP server or domain controller without prior permission from the Information Security Team.[Severity: Medium]
d. In some projects, Cybage employees may have access to computers or devices that are not part of the Cybage network. Such network may be the customer's network or other network that the customer may require Cybage employees to work upon. Such networks may not have the same level of restrictions that Cybage network has. Employees must use such networks, computers, devices for work related purpose only. [Severity: high]
e. VPN access to Cybage network will not be provided by default. It will only be available upon request to onsite employees, employees working in staff augmentation projects and to employees at level 3 and above. [Severity: NA]
f. Network Security key used for connecting to wireless networks will not be provided to anyone. For security reasons, this key is kept with the IS dept. only. [Severity: NA]

9. Software

Using software diligently not only reduces the unnecessary use of licenses but also reduces performance and security issues and reduces maintenance related activites such as installing security patches and service packs.

9.1 Acceptable Usage:

a. Employees can install, on their own, software available at \\ct-share\UtilitiesforAll. For all other software the employee must log a ticket under helpdesk. [Severity: Medium]
b. Employees should not download or store software installers on the machines. [Severity: Medium]
c. If unauthorized software is found stored or installed on an employee's machine then the employee may have to compensate for the commercial loss that Cybage may bear arising out of such malpractice. This is in addition to the action that the user will face as defined under the Disciplinary Action section in this document. [Severity: Medium]
d. Employees must not tamper with any service or application that is deployed by the IS Department. Such software includes but is not limited to antivirus or PC monitoring application. [Severity: Medium]

e. Employees should not install on their user machine any software that binds to the installed hardware. Installing such software on another machine may have licensing implications. Employees should discuss with the IS department for an alternative solution. [Severity: NA]

f. In continuation to point 6.1.5 above, employees should not use their user accounts for any setup. This may create dependency upon the user account and may cause inconvenience to the project if the user account is deleted as part of the employee's exit formalities. Employee should request for a service account and use it instead. [Severity: Low]

g. Project managers have to define in MIS, all applications that are required for their project. [Severity: NA]

h. The software compliance audit that the Information System team carries out, treats a virtual machine in the same manner as a physical machine and thus all clauses related to the audit of a physical machine apply equally to the virtual machine [Severity: NA]

i. If an employee is working for more than one project simultaneously then the employee can request applications that are listed in either of the lists for the projects. [Severity: NA]

j. If the project uses any software that the customer has supplied for use within the project, the PM should contact the Legal team (legal_team@cybage.com) and complete the formalities before adding the software in the list on MIS. This is required because certain software are not permitted to be used beyond the boundaries of the region of purchase. [Severity: Medium]

k. Software installers or licenses must not be stored on the project repository (version control systems) even if it is required for the project or provided by the client.[Severity: Low]

9.2 Software Lab

A software lab has been set up in case an employee requires to install and evaluate a software. No approvals are required for software evaluation in the software lab.

a. Users must install and test Trial/Evaluation software in the Software lab only and not on the user or project machines. [Severity: Medium]

b. Use of crack/pirated version of software or illegal software is strictly prohibited even in the software lab. Only freeware, shareware and evaluation versions of software may be installed. [Severity: Medium]

c. User should login to the machines in the software lab with their domain login accounts. [Severity: NA]

d. Users should log off once he/she is done using the machine. [Severity: NA]

e. The Cybage network is not accessible from the lab. [Severity: NA]

f. In case the user requires using the machine over an extended period of time and doesn't wish for the machine to be restarted or formatted, he/she should leave a note accordingly on the white board. [Severity: NA]

g. The machines in the software lab are to be used on a first-come-first-serve basis and the IS team will not be responsible for reserving/blocking machines on behalf of the users. [Severity: NA]

h. The IS team will not be responsible if anyone reboots/formats the machine despite your note on the white board advising against it. [Severity: NA]

i. Internet usage would be restricted only to technical sites. Access to other categories such as webmail, social networking, and banking sites would not be provided and such requests will not be entertained. Internet Kiosks should be used for such activities. [Severity: NA]
j. Downloading/browsing bandwidth will be provided on a best effort basis in the software lab. [Severity: NA]

10. Hardware

10.1 Acceptable Use of hardware:

a. Cybage shall be the owner of the hardware and IT infrastructure provided to the employee for work. The employee shall only be the consumer of the hardware and IT infrastructure. Cybage shall have exclusive right to monitor and alter the hardware and IT infrastructure provided to the employee for work, at its own discretion, and as per the prevailing policy. [Severity: NA]
b. User is accountable for all the hardware provided by the organization. Any damage due to unintentional or intentional mishandling will be the user's liability. In such cases the cost of repairing or replacing the hardware will be recovered from the user which will be in addition to the disciplinary action taken against the user as explained in this policy. [Severity: NA]
c. Employees must not bring any personal hardware or media inside Cybage premises. Personal hardware includes, but is not limited to, USB drives, cameras, CD/ DVDs, MP3 players, laptops etc. The only exception to this is headphones. A fine of Rs. 250/- would be levied from the user if the confiscated device is returned to the user. [Severity: NA]
d. Employees must not carry out of the premises, any hardware that is owned by Cybage or Cybage's customers. [Severity: High]
e. Users should not swap/ exchange or shift any hardware amongst them. [Severity: Medium]
f. Users should switch off their machines and other hardware devices before leaving for the day. [Severity: Low]
g. If employees are expected to be out of office for more than a month, they should return their machine and other hardware devices to the IS department [Severity: NA]
h. Any hardware received from the client or purchased on behalf of the client must be informed to the IS Infrastructure team for inventory related formalities. [Severity: low]
i. In case the hardware needs to be returned to the client, the concerned project manager should inform the IS infrastructure team which would then release the same from the inventory system. [Severity: low]
j. Speakers must not be used in cubicles.[Severity: Low]
k. Employees at level 6 and above are eligible for a personal printer which would be provided on request. [Severity: NA]
l. Users should not store any audio and video files on their computers. IS team will audit your computer and remotely delete any such files without your permission if they are found on your computer [Severity: medium]

m. The only exception to this clause will be client recordings and any walkthroughs provided by the client.[Severity: NA]

n. If any of these audio/video files received by the client requires a license, then the same should be routed through the legal team (legal_team@cybage.com) before these files are used. [Severity: medium]

10.2 Acceptable use of Laptop

a. Laptop is permanently issued only to employees at Level 5 and above. [Severity: NA]

b. Laptop is issued on a temporary basis to users who are travelling for official reasons. It will be made available on a best effort mechanism.[Severity: NA]

c. Laptop should be returned within 2 working days after returning to office from an onsite visit. [Severity: Low]

d. User returning from onsite visit should ensure that the laptop is audited by the Information Security Team before connecting it to the network. [Severity: Medium]

e. Laptops issued on a permanent basis will be audited randomly. [Severity: NA]

10.3 Machine issue and release

a. Computers will be provided with the standard operating system which is Windows 7 Enterprise. [Severity: NA]

b. CD-ROM or DVD-ROM drive will not be provided with the machine. [Severity: NA]

c. The following convention should be followed while setting up the machine name

- Machine name should be the same as the user's login name followed by a hyphen (-) with the OS type, for e.g. if the user's login name is *Amitdh* the machine name can be *AMITDH* or *AMITDH-WIN7*. Other examples for other OS are *AMITDH-WIN2K3*, *AMITDH-LINUX*. [Severity: Low]
- A central system in the project other than user machine should have the machine name assigned as *projectshortname-serverpurpose* for e.g. machine used as VSS in the MIS project will be *MIS-VSS*[Severity: Low]
- A test machine in the project should have the name assigned as projectshortname-test-OSshortname, for e.g. machine in MIS project should be assigned name as MIS-test-Win2k3 or MIS-test-Ubuntu. For multiple test machines a number should be appended to its name[Severity: Low]

d. User will have to return hardware assets to the IS Department immediately upon change in project, project closure or upon the user's exit from the organization. No formalities related to project closure, employee release from a project or employee exit will be completed unless the machine is returned. [Severity: NA]

10.4 Machine Shifting

a. Shifting is mainly of 2 types :

- Shifting within the project: Only IT assets such as user's machine or the project test or server machines will be shifted from old location to new location within the same project. [Severity: NA]

- Shifting due to change in the project: Whenever there is a change in project, the user will be issued a new machine. Data from the old machine will be transferred to the new machine only after it has been approved by the PM in the old project and by the Information Security team. The old machine has to be returned to the IS Infrastructure team. This is applicable even if there is no change in the user's physical location. [Severity: Low]

b. While transferring data from the old project, only personal data limited to salary slips, project photos, books, tutorials and assignments are allowed for transfer. [Severity: high]

c. Before logging a request in helpdesk for shifting, the user should ensure that the new location is free by checking with the Infrastructure team. [Severity: NA]

d. Whenever there is an inter-office transfer from one city to another, with or without change in project, users will have to return the machine before leaving the old location and will be allocated a new machine at the new location. [Severity: low]

e. All users who have logged a request for shifting will be informed about the shifting in advance by email. Users should ensure that they shut down their machines before shifting scheduled. If the machine is left on, the IS team will switch off the machine and will not be responsible for any loss of data or work. [Severity: NA]

f. IS Team will shift only the IT assets. [Severity: NA]

g. Shifting will be scheduled only if it is approved by the respective Manager or Delivery Manager or Delivery Head of the project. [Severity: NA]

h. SLA for regular shifting is one day. It will differ according to shifting category:

- Shifting within same A/c will take place in a day's time once the seat confirmation is done.
- In case of shifting with change in A/c, it will be done on next day after data backup is done.
- Bulk shifting will be carried only on weekends.

11. Acceptable usage of Central resources

Central resources are those that are available at all times, like common printers, scanners, public share, etc.

11.1 Printers

a. Users should only print official documents. [Severity: Low]

b. Common printers are available on every floor at each facility. Users should install the printer available on the floor at the facility where they are located. To install the printer please refer to 'Printer Installation' document on http://cybintranet -> IS -> News and Announcements[Severity: NA]

c. Employees at grade 4 and higher grades may print unrestricted number of pages. All other users have been given access to print 10 pages per week. [Severity: Low]

d. Users must collect all documents that they print. Users who do not collect their documents by the end of the day will be liable to disciplinary action as described at the end of this policy. The level of severity of the policy violation will be decided based on the nature of the printed document. [Severity: Low/ medium]

e. Users must destroy any unwanted printouts using the paper shredders that are provided near every printer. [Severity: Low/ medium]

f. For color printouts, a request should be logged in IS helpdesk. [Severity: NA]

11.2 Public share

a. Public share should be used only for sharing official data within the company. [Severity: Low]

b. User can copy data only up to 7 MB in a single folder on the Public share. [Severity: NA]

c. Certain file types (audio, video and executable) should not be copied to the public share[Severity: Low]

d. After creating a folder under the public share, the creator has to give explicit permissions to his own user account and other users requiring access to it. [Severity: NA]

e. Contents under public share will be deleted every day at 07:00 AM IST, using an automated script. [Severity: NA]

f. This folder is not included in the backup cycle. Users are requested to maintain a copy of the data that they are sharing. [Severity: NA]

11.3 Scanner

a. Scanner may be used to scan official as well as personal documents. [Severity: NA]

b. Scanner is available in the internet kiosk. [Severity: NA]

11.4 Conference Rooms

a. Conference rooms booking facility is available on CybageMIS portal under Information Systems

b. Conference room machines will have only basic software like Microsoft Office, Acrobat reader and the application required for call recording. [Severity: NA]

c. Users will have access to their machine from conference rooms only over Remote desktop. While setting up the user machine to receive the remote connection from the conference room machine, the user should select the option “Allow connections only from computers running Remote Desktop with Network Level Authentication” under Remote Desktop. [Severity: NA]

12. User accounts / passwords

a. Four types of user accounts are created depending upon the requirement. [Severity: NA]

- User User account: Should be used for day-to-day activities like logging in to the machines. This user account and an associated email account is created when the user joins the organization and only as per the username given by the HR department.
- User account for client: Is provided only to Cybage’s customers and visitors. This account will be issued on request via helpdesk and will be valid only for a specific period. No email account is created for this type of user account.
- Test account: Is created for the purpose of testing in the project. This account will be issued on request via helpdesk and will be valid only for a specific period. No email account is created for this

type of user account. Service account: Is created for special purposes where the account will be used by services or applications. The password for this account never expires. No email account is created for this type of user account.

b. Password policy with following conditions is technically enforced-

   1. The password will be valid for 45 days
   2. The password should contain minimum 8 characters
   3. Password once set cannot be changed in the first 5 days.
   4. Users are not allowed to repeat their last 5 passwords
   5. Password should not contain three or more characters from the username
   6. The password should contain characters from three of the 4 categories mentioned below.
      a. lowercase letters
      b. uppercase letters
      c. numbers
      d. Special characters

d. The password expiry warning mails for domain user accounts start 7 days before the password expires. [Severity: NA]
e. Password should be changed at regular intervals as defined in the password policy. In case the password expires due to user negligence, the user will have to meet the Information Security team for resetting the password. The Information security team will reset the password only after the user shows the Cybage ID card [Severity: NA]
f. Passwords, after resetting, will not be informed verbally. [Severity: NA]
g. Users should ensure that they use strong passwords on all systems. [Severity: NA]
h. To reset password for onsite users or users located at other facilities or users on leave, the respective project manager should log a helpdesk request or should send a mail to Information security team (security@cybage.com). The new password will be provided to the project manager or the respective DM/DH only over their Cybage mail ID. [Severity: NA]
i. Password must never be disclosed to anyone or written on documents or be stored in files on a computer that can be easily accessed. [Severity: Medium]
j. Users are responsible for protecting their passwords and mail ids. Users will be held accountable for all system activities that are carried out using their ID. [Severity: Medium]
k. User account will be locked out after 4 incorrect logon attempts made over a period of 2 hours. [Severity: NA]
l. If the user account is locked out, it would remain locked for a period of 2 hours. The user account will be automatically unlocked after this 2 hour period expires. [Severity: NA]
m. The user can either request his manager to route the request via IS Helpdesk “password reset” category to unlock the account / reset the password or attempt to login again after 2 hours. [Severity: NA]
n. Users must not try another user’s account password with the intention of causing it to be locked out as this could lead to productivity loss or disrupting services linked with that user account. [Severity: Medium]

13. Helpdesk

The Helpdesk application is designed specifically for Cybage employees to log requests directed to the support departments like Information Systems, Human Resources, Admin, Finance, Intranet, QMS etc. Helpdesk can be accessed using the link http://newhelpdesk.cybage.com.

a. Users should ensure that they select the appropriate category while logging a case in helpdesk. Helpdesk requests with incorrect or incomplete information will be returned to the users to make the necessary corrections. [Severity: NA]
b. Users should raise separate tickets for every issue that they face. In case any user is not able to log a helpdesk request from their machine due to some problem, they should log a request from a machine in a conference room or should request their colleague to log a request on their behalf. [Severity: NA]
c. For a request where an exception will have to be made to an existing policy, user will be able to raise a ticket with a maximum validity of six months. The user will have to raise a new ticket to continue with the privileges before the validity period has elapsed. [Severity: NA]
d. IS Helpdesk is available on working days between 09:30 AM to 06:30 PM. [Severity: NA]
e. Each request has a pre-defined resolution time which is mentioned in the helpdesk ticket logged by user. Users should refrain from calling the IS helpdesk for updates on their tickets till the resolution time has been crossed. [Severity: NA]
f. For any critical issue which is required to be handled on priority, user should ask his manager to send a mail to the Manager_IS DL. [Severity: NA]
g. Tickets will be hibernated in case of a dependency. For e.g. Hardware not available. [Severity: NA]
h. Users can re-open the ticket only if the problem re-occurs within 10 days of closing the ticket. [Severity: NA]
i. Response time is the time taken by the IS coordinator to screen the ticket and assign it to the IS engineer (this is defined as 30 min). User gets an automated response once their request is assigned to an engineer and same applies whenever the ticket is updated and closed. [Severity: NA]
j. Tickets that require approval will not be worked upon unless it has been approved by the concerned manager. In such cases, the resolution time starts from the time the ticket is approved. [Severity: NA]
k. Helpdesk system will not be available over the Internet. Users who need assistance when onsite or when they are travelling can raise a helpdesk ticket through SSL VPN or drop a mail to the IS team. [Severity: NA]

14. Remote Connectivity

Remote connectivity is allowed to Cybage network using the SSL VPN service. This access is not allowed by default but is enabled for users who are eligible. Employees at Level 3 and above, users travelling to or stationed at client's premises are eligible to connect remotely to Cybage network via the SSL VPN.

a. A default policy is created for Cybage users through which they will have access to the resources mentioned below. [Severity: NA]
    - Helpdesk

- TTPRO
- Timesheet
- QMS Quiz
- Intranet
- QA Wiki
- CybageMIS
- Appraisal System
- Investment Declaration form
- All other Cybage MIS services

b. Resources available through the SSL VPN may change from time to time without any advance notification. Changes will be updated and communicated to everyone accordingly. [Severity: NA]
c. In case any access other than what is mentioned above is required, the user will need approval of the CTO and the Information Security Team. [Severity: NA]
d. In case a client needs access to a particular machine, URL, etc. in the Cybage network, approval of the project manager of that project, the CTO and the Information Security Team is required. [Severity: NA]

15. Users on H1 or at Cybage Inc

Employees on H1 or those being transferred to Cybage Inc. facility for long period need to follow this policy

a. All formalities relevant to the laptop issue for Cybage Inc. should be done from the Cybage Pune office. [Severity: NA]
b. Users moving to Cybage Inc. should raise a laptop request at least 4 days prior to their travel and should mention all relevant information pertaining to the laptop in the request. The user will be required to return their existing desktop/laptop to the Cybage Infrastructure team. [Severity: NA]
c. In case a laptop needs to be procured by the user directly, he/she should get an approval from the concerned Delivery Head and all relevant details should be provided to the Infrastructure team at Pune, who will then inform the Cybage Pune finance team accordingly. Original receipts have to be submitted at the Cybage Inc. office to claim reimbursement. [Severity: NA]
d. In case of any technical issues with the laptop provided, the user should contact the IS team at the Pune office immediately. [Severity: NA]
e. In case a user at Cybage Inc. resigns, he should send the laptop to the Cybage Inc. Redmond office or should make arrangements to have the laptop sent back to the Cybage Pune office. [Severity: NA]

16. Data & Source code Security

a. Users must refer to the classification of information before sharing data with anyone. The classification decides who you can share the data with. Any exception to this will be treated as a

case of data leakage. Kindly refer to the table below to understand information classification and the associated persons who are authorized to view the information. [Severity: High]

Classification	Explanation	Effect of unauthorized disclosure, compromise or destruction	Example of information
Public	Information can be disclosed to anyone. Knowledge of this information does not expose Cybage to financial loss, embarrassment, or jeopardize the security of Cybage's assets	No effect	Marketing brochures, Published annual reports, Interviews with news media, Business cards, Press releases, Web pages and web content, Published financial information etc.
Internal	Due to its technical or business sensitivity, information classified as *Internal* is limited to Cybagians, contractors, Clients and vendors covered by agreements.	Minimal or no significant impact to Cybage, its clients or employees	Employee Handbook, Telephone Directory, Organization Charts, Policies, Routine administrative & office information, Security awareness training materials etc.
Departmental	Information classified as *Departmental* is intended solely for use within the department / process and is limited to those with a business need-to-know including CXOs, VPs, DM/DH and the clients.	Directly or indirectly have an adverse impact on the department / process and to its clients or employees. Financial loss, damage to Cybage's reputation, loss of business, and potential legal action could occur.	Software, Hardware & System specifications & Configurations, Network Diagrams, Proprietary Software, Client records & correspondences, Business plans, Budget information, Security Plans & Standards, System & application passwords, Security audits and logs, Personnel records (payroll) etc.
Confidential	Information classified as *Confidential* is intended solely for restricted use within Cybage and is limited to those with an explicit, predetermined business need-to-know.	May cause severe damage, provide significant advantage to a competitor or cause penalties to Cybage, its clients or employees.	Strategic plans, Encryption keys, Information on legal proceedings, Administrative passwords etc.

b. Users must not engage in any unlawful activity such as trying to access unauthorized information or resources, hacking, introducing any computer virus or malware or committing acts that may disrupt use of resources[Severity: High]
c. Users should not share any content on their machine unless it is required for the project. In case content needs to be shared then it should be shared only for specific users with appropriate

permissions such as read, write. Content should not be shared for everyone or full control permissions should not be assigned[Severity: Low]

d. Users must not post the project source code, in part or full, on the internet or share the same with other projects or users within or outside Cybage[Severity: High]
e. Users must not use, in part of full, in the source code in their project, any source code belonging to any other person or blog available on the Internet or other projects running in Cybage . [Severity: High]
f. Source code should only be transferred on a secure channel such as but not limited to VPN, secure FTP, encrypted email (if provided by the client). Source code should not be transferred over email in clear text, regular FTP or chat application. [Severity: Medium]
g. Users should ensure that local copies of source code should be present on their systems only until the source code is checked in and should be destroyed after that. [Severity: NA]
h. Users should not forward business sensitive emails originating from either Cybage or customer domains to any free public email domains such as but not limited to yahoo, hotmail, etc. [Severity: Low]
i. Users should not use their personal email addresses as contact addresses for conducting Cybage business operations**[Severity: Low]**

17. Disciplinary Action

- Policy violation is categorized according to severity as low, medium or high.
- If found to be a defaulter the Cybage Information Security Team will issue an official warning through mail keeping the project manager , delivery manager / delivery head in loop
- If found to be a defaulter for the second time (medium severity), Cybage Information Security Team will escalate this to the HR Department & the Management team for decision on further action. This may lead to one day gross salary cut.
- For high severity policy violations, Cybage Information Security Team will escalate the matter to the HR Department & the Management team for decision on further action. This may lead to suspension or termination of services of the defaulter and/ or legal action as deemed fit by the Company.

Note: Kindly refer to the **Disciplinary process** available at CybIntranet → Process → QMS → Departmental Manual → Human Resource (HR) → Disciplinary Action Process

18 Rights, authorities & permissions

- The IS team reserves the right to question any user for any non-compliance in the implementation of the policy
- The IS team reserves the right to audit any machine at any time without the user's permission or knowledge.
- The IS team reserves the right to disable any account, delete or hold any objectionable material from any machine which may be used as evidence.

- Exceptions to the policy clauses mentioned above will be treated on a case-to-case basis and will be made for a period of 6 months only.
- At any time and without prior notice, Cybage information security team reserves the right to examine un-official file directories, emails and any content which is stored on any Company owned device.
- Disclosing confidential or proprietary information, by the employee will result in regulatory violations for the organization or its existing or prospect clients. If done so, it will call for a disciplinary action against the employee.
- Cybage reserves the right to monitor online blogs, social networking sites accessed using company IT infrastructure and interfere legally, if required, considering any content posting which is not in compliance with this policy and violates the Confidentiality of the Company Data.

Employee Code _____

Name _____

Signature _____

Date _____

NOTE: This policy in its latest form is available at https://cybintranet -> IS->IS Policies->Information Security Policy.

Employees are requested to go through the complete policy and ensure compliance at all times.

Any additions and / or alterations to the policies will be reflected in this document and will be informed to everyone. If you have any questions / concerns regarding information security, please contact the Information Security team at security@cybage.com

19 Review frequency:

This policy is reviewed yearly.