	STAR E PROCESSORS	Doc.Ref.SEP-P-16
	Arang, Raipur, C.G (492101) India	Rev #01 Dt 01.01.2021
	Data Security Policy and Incident response procedure	Section 2

1. Objective	To lay down a Data Sanitization Plan for data contained equipment, component and materials dealt in SEP recycling operations
2. Scope	The procedure is applicable for SEP recycling operations only
3. Responsibility	Top management, EHS Coordinator and process wise personnel
	1. Office Computers and Server: There are some truths that should be self-evident but need to be spelled out in a written policy, because inevitably an employee will otherwise do the unthinkable. Some may ignore the Not Safe for Work (NSFW) tag and view pornography if they are 'off the clock' during a break or lunch hour, while others may decide to run a personal business or game server using the firm's servers. Both of these activities expose the office to security risks. Some less obvious but equally risky behaviour is the desire to download software from the internet onto company computers and/or servers. An employee could simply be looking for a tool to make them more efficient in their job. However, looking in the wrong place and downloading the wrong file could install malicious software onto your system. Perhaps the scariest danger is the easiest one to complete: deleting files. Deleting a file can sometimes be as simple as hitting the wrong key combination, resulting in a mad dash to the IT specialist with the order to "retrieve!" said file from the trash bin. On those occasions that the deletion wasn't noticed right away, IT can spend a significant amount of time with the backup locating the document to hopefully restore it. To prevent these and other related computer and server nightmares, create an acceptable use policy as part of your data security package. Restrict who has the right to download executable files (programs) and who can modify items in certain folders. Firewalls, virus scan and anti- spam software should be installed, updated and the system regularly scanned. **2.Secure Backups:** Is losing a day's worth of work acceptable, let alone a week? Backing up the office servers every night and storing that data off-site can save a law firm. Disasters don't wait for you to be prepared before they strike. Servers, like other computers, can die without warning. Having a full backup available allows you to upload your data onto a new server (after a new server is acquired and built) and continue working without having to reinvent lost work. It's even better when you have a redundant system, and you can simply switch to your backup server and continue on as if nothing has happened. There are different varieties of backup systems available. Cloud backups remove the need for equipment but require extra vigilance regarding security when selecting a company. USB backups give the convenience of a portable backup, but proper security must be maintained since they are small and easily lost. Older tape backups require special equipment, someone diligently managing the process, and secure storage.

When planning your backup system, budget may be a factor in deciding which route you take. However, you have to pick a system you will use. Saving money isn't a value if it's tedious work that never actually gets done and you don't have a current backup when you need it. Your backup policy should include determination for how long backup copies will be kept. Additional USB drives can be purchased to maintain offsite backups. If using the tape system, have a series of tapes that you rotate. Because tapes deteriorate, replace them on a regular basis to prevent problems. Keeping end of month or end of year backups offsite may be helpful as well.

3.Password Security:

Recent headlines highlight the continued problem of creating simple passwords that are quickly hacked because they are easier to remember. If a site requires a complicated password, some people will write it down and attach the post-it note to their computer so they have easy access to it when they need it. Others save a document in the system with their list of passwords to various sites. Any of these methods are hazards that can provide unauthorized access to your system. To combat the dangers of password accessibility, provide minimum requirements of at least eight characters and combinations of the following: lowercase letters, uppercase letters, numbers, and special characters. Simple common words or the individual's name and date of birth shouldbe prohibited. Provide some examples of possible strong passwords that would be easy to remember, such as word combinations (previous addresses: Main#202ParkDrive). Passwords should be scheduled to be changed on a regular basis, and passwords should not be able to be used over and over again in succession. In addition to making sure individual passwords are truly secure, be sure that the system passwords for wireless access and other equipment are also changed. These hidden passwords can open up the entire system to hackers even if you think you've created a secure system with layers of access.

4.Internet Use:

Preventing employees from ever surfing to a nonwork-related website can be cost prohibitive for small and medium sized firms. However, having a clear internet use policy can help limit the types of sites they visit. Streaming music and video use a lot of bandwidth, and downloaded files from filesharing sites can contain malware or expose the firm to liability if material was copyrighted. Some employees may be tempted to spend too much time on activities such as online shopping, social media or travel planning, Again, use the theory that if it isn't forbidden, they will do it. Specifically list any types of sites that you do not want your employees visiting on your office computer. Security settings can be set to block porn sites, gambling sites, social media and even web based email sites. The

logic behind blocking personal, web-based email is prevention of employees from opening emails and visiting a nefarious site or opening an infected attachment, thereby compromising your system because their personal email was not as secure. Employees may inadvertently or maliciously transmit client confidential or law firm proprietary information using their personal webmail, circumventing other safeguards the firm has established concerning such information. Remind employees that, like email, browsing history is subject to being reviewed.

5.E-mail:

Misuse of company email is one of the most common problems faced, and covers a large variety of actions. Sending a free “Happy Birthday!” card from a free website can introduce massive spamming into your system and bog down your server. Employees may use company e-mail for running a personal business with less thought than storing hard files on the computers or servers. A good Samaritan employee may send out emails to everyone in the firm regarding a fundraising event for a local charity, and follow up with four or five reminders. Personal use of the firm email system should be addressed to reduce the amount of server space such items consume. E-mail policies should also include limits on the size of attachments as appropriate. Consider this: an e-mail with a 10MB attachment is received and then forwarded to ten other employees. This attachment now consumes 120MB of server space as each individual copy of the e-mail is stored on the server, plus the copy in the sent folder. Depending on your e-mail client, a copy of the e-mail may also be stored on each and every computer. The above space consumption issue illustrates the reasoning behind another policy: e-mail retention policy. Case-related e-mails and attachments should be uploaded into a practice management system or database, protecting them from accidental deletion and making them accessible to all employees who may need the information. Storing emails that need to be saved outside of the e-mail system also prevents the dreaded moment when the recipient is out of the office and IT has to search their e-mail so another employee can access the information. An essential element of an e-mail policy is reminding employees that the office email system is firm property and not their personal account. As such, any office email account is subject to review. Remind employees that office e-mail is representative of the firm and should present a professional image.

6. Metadata:

Perhaps the most overlooked data security danger is metadata contained in document editing programs. Both Microsoft Word and WordPerfect contain information regarding previous edits made to a document. This means that deleting confidential information from one client document to reuse for another could expose the former client’s information to the latter if the recipient knows where to look. These features can be turned off,

preventing data from being stored in the first place. Files sent electronically should be scrubbed for metadata. Special programs can be purchased to ensure that this information is not forwarded along with your document and can be integrated into your email system. If you do not want the recipient to make changes to your document, send the document as a PDF. Sending as a PDF strips most of the metadata from a file, but a PDF contains some of its own. Be sure to adjust the security options as appropriate.

7. Remote Access:

Employees may need to access the firm's system when they are out of the office occasionally. Prohibiting employees from using public computers or using wireless access in public places removes the exposure of client data from hackers because security settings in these circumstances are often lower than those created for the office. To make connecting to the office more secure, consider establishing a virtual private network (VPN). A VPN connects you to your office computer over the internet, alleviating the need to actually access files through a questionable internet connection. Communications sent through the VPN are encrypted, so any data intercepted would not be usable.

8. Smartphones, Tablets and Remote Storage Devices:

The trickiest part of data security is protecting the mobile data that leaves the building. Smartphones and tablets all contain internet connections but often do not have all of their security measures activated as a firm laptop would provide. A USB drive often contains pure, unencrypted files available for anyone who plugs the drive into their computer; worse yet, it is small enough to easily lose. Any device used to access client data should have password protection requirements. Even a USB device can be purchased that requires password access. For smartphones and tablets, require passwords at start up and after a period of idle time. Also, develop a remote wipe program protocol should any device ever be lost or stolen. Any document downloaded and stored should be encrypted. When travelling, be careful not to leave your device in 'airplane mode' as this often disables the ability to enact a remote wipe program as it disconnects the device from data systems used to locate it. Upon return to the office, require that remote storage devices such as USB and flash drives be scanned by virus and malware scanners to prevent infection from any outside sources. Have protocols in place regarding the use of personal USB devices with office computers to avoid inadvertently infecting office computers with unprotected devices. Consider restricting access to USB ports to certain employees, or even disable ports to prevent misuse. " The trickiest part of data security is protecting the mobile data that leaves the building. Smartphones and tablets all contain internet connections but often do not have all of their security measures activated as a firm laptop would provide.

	9. When an Employee admits to duties and Leaves: Upon permitting the employees in deploying their roles, responsibilities a Non-Disclosure statement of data be obtained from employees not disclose any of the data information to persons other than company working personnel designated for. Often the biggest threat to your data is within your own company. A disgruntled or exiting employee can easily delete files from your system or take files out of the office without notice. Locking down data from employees can be the hardest part of data security. When an employee leaves, immediately lock their computer, e-mail, remote access and any other access privilege to prevent them from accessing information. Create protocols within the firm for who may need to access an employee's files. If the employee has any equipment, such as a laptop or USB drive, at home, verify that it is returned before they exit the premises on their final day. **10.Visitors and Contractors:** From time to time, office visitors may need to use office computers or email. Any temporary account established should have a notice regarding expectation of privacy. Passcodes for these accounts should also expire immediately after use. This ensures someone temporarily allowed into your system won't be able to access your confidential data later, when you're not looking. System contractors obviously need access to keep everything up-to-date and running smoothly. However, they may not understand the importance of the confidentiality of the information they may access in the process of completing their work. A Vendor/ Contractor Confidentiality Agreement should be completed by all of those who will be accessing your system to ensure that confidentiality is maintained. **11. Security Audit:** To ensure all facets of your system are properly secure, consider a 1st party security audit done by trained professional Internal auditor in internal audits done once per 6 months as part of Internal audits will see any holes in your protection that could leak confidential information. The auditor will be able to provide you with suggestions to improve your security to prevent data security breaches in the future. This may include the purchase of additional security software, or simply changing internet usage habits. The end result will be a safer practice. **12**. In case of failing in implementing and maintaining points 1 to 11 then a Data incident report be initiated and corrective action in the same be ensured within the time frames agreed for.
Records	Data Incident Record