Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the likelihood of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
1. Photocopiers	Internal Hard Disk Drive	Any photocopier built after 2002 contains an internal hard disk drive. This hard drive stores copies both in JPG and PDF format of every scan, email and fax sent from that machine. The data stored on photocopiers cannot be classified as low or high sensitivity as there is no way of identifying what jobs have been processed by the device. This means the whole device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organisations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitive proof that the data on every photocopier has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every photocopier disposed of: Follow Control Process 1 & 3 & 4 & 6 & 8 & 9 & 10	High	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
2. Multi-Function Printers	Internal Hard Disk Drive	Network printers and multi-function printers that have the ability to ether scan, fax or email documents sent to them have built in hard disk drives. The reason for this is that data sent to a MFP has to be converted to an image or pdf file and stored in order to be emailed or faxed. What organisations do not realise is that this information can be stored for a very long time until it is overwritten by another set of images. An example:- A typical 1 page pdf file is approximately 100kb. On a small 40GB HDD this would equate to over 4 million stored scans before any are overwritten. The data stored on multi-function printers cannot be classified as low or high sensitivity as there is no way of identifying what has jobs have been processed by the device. This means the whole device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data on every Multi-Function Printer has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Multi-Function Printer disposed of: Follow Control Process 1 & 3 & 4 & 6 & 8 & 9 & 10	High	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
3. Network Routers	Internal Flash Drive Configuration	Network routers are the gateway from your organisation to the World Wide Web. They hold information about your organisations external IP address, port numbers, user names, passwords and even site-to-site encryption settings. An outside body with this information can rapidly gain access to your internal systems and produce a number of malicious attacks or data breaches. Access to internal configuration of the most popular network routers is easy to gain once you have possession of the equipment though a console cable linked to a standard laptop. This means the whole device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data on every Network Router has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Network Router disposed of: Follow Control Process 1 & 3 & 4 & 5 & 6 & 8 & 9 & 10	Medium	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
4. Firewalls	Internal Hard Disk Drive	The vast majority of commercial firewall equipment contains a hard drive. By simply pulling the HDD and running some easily available forensic software, people can access a vast amount of information stored on this drive. The drive stores information in relation to IP addresses and port numbers both internal and external as well as email addresses, telephone numbers and user ID's. Email routing information is very valuable to "Phishing" schemes and firewalls contain all this information for your business to be targeted. This provided to the wrong hands would not only constitute a serious data breach, but could also open a gateway to malicious attacks. This means the whole device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data on every Firewall has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Firewall disposed of: Follow Control Process 1 & 3 & 4 & 5 & 6 & 8 & 9 & 10	Medium	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
5. CCTV Systems	Internal Hard Disk Drive	All CCTV Systems contain hard drives that store recorded camera information that is overwritten by new images over time and dependent upon the size of the hard disc drive, this could be up to 2 weeks of sensitive images. There are very specific Data Protection Laws governing viewing and access of CCTV footage. Including, but not limited to, human rights privacy laws. This means the whole device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every CCTV System has been destroyed needs to be ob-tained. The following Processes ensure 0% risk is achieved for every CCTV System disposed of: Follow Control Process 1 & 3 & 4 & 5 & 6 & 8 & 9 & 10	High	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
6. PC's	Internal Hard Disk Drive Overlooked CD/DVD Overlooked Flash Memory Overlooked Floppy Disc Overlooked Backup Tape Overlooked Zip Drive Possible Multiple Hard Drives	Internal PC hard disk drives are becoming larger and larger. With an average of 512GB per PC that is an immense amount of company documents, settings and potentially confidential information. Every document, JPEG, PDF, Excel sheet you view is stored in a temp folder regardless if the item was "saved". All this information is available to somebody intent retrieving it. On many occasions CD/DVD's with live sensitive data are inadvertently left within the CD/DVD Player of the PC if it contains one. On Many occasions Flash Memory with sensitive data is left within the Memory Card Reader of the PC if it contains one. On Many occasions Floppy Discs with sensitive data are left within the Floppy Drive of the PC if it contains one. On Many occasions Backup Tapes with sensitive data are left within the backup Device of the PC if it contains one. On Many occasions Zip Drives with sensitive data are left within PC if it contains one. Many modern PC's have multiple hard disc drives, identification, tracking and correct destruction of additional drives can easily be over looked.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every PC has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every PC disposed of: Follow Control Process 2 & 3 & 4 & 6 & 7 & 8 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
7. Laptops	Internal Hard Disk Drive Overlooked CD/DVD Overlooked Flash Memory Overlooked Floppy Disc Possible Multiple Hard Drives	Internal Laptop hard disk drives are becoming larger and larger. With an average of 512GB per PC that is an immense amount of company documents, settings and potentially confidential information. Every document, JPEG, PDF, Excel sheet you view is stored in a temp folder regardless if the item was “saved”. All this information is available to somebody intent retrieving it. On many occasions CD/DVD’s with live sensitive data are inadvertently left within the CD/DVD Player of the PC if it contains one. On Many occasions Flash Memory with sensitive data is left within the Memory Card Reader of the PC if it contains one. On Many occasions Floppy Discs with sensitive data are left within the Floppy Drive of the PC if it contains one. Many modern Laptops have multiple hard disc drives, identification, tracking and correct destruction of additional drives can easily be over looked.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Laptop has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Laptop disposed of: Follow Control Process 2 & 3 & 4 & 6 & 7 & 8 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
8. Servers	Internal Hard Disk Drive Overlooked CD/DVD Overlooked Flash Memory Overlooked Floppy Disc Overlooked Backup Tape Overlooked Zip Drive Possible Multiple Hard Drives	Internal Server hard disk drives are becoming larger and larger. With an average of 512GB per PC that is an immense amount of company documents, settings and potentially confidential information. Every document, JPEG, PDF, Excel sheet you view is stored in a temp folder regardless if the item was “saved”. All this information is available to somebody intent retrieving it. On many occasions CD/DVD’s with live sensitive data are inadvertently left within the CD/DVD Player of the PC if it contains one. On Many occasions Flash Memory with sensitive data is left within the Memory Card Reader of the PC if it contains one. On Many occasions Floppy Discs with sensitive data are left within the Floppy Drive of the PC if it contains one. On Many occasions Backup Tapes with sensitive data are left within the backup Device of the Server if it contains one. On Many occasions Zip Drives with sensitive data are left within the Server if it contains one. Many modern Servers have multiple hard disc drives, identification, tracking and correct destruction of additional drives can easily be over looked.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Server has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Server disposed of: Follow Control Process 2 & 3 & 4 & 6 & 7 & 8 & 10	Extreme	Zero	Low Risk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
9. Cameras	Internal Flash Memory and Removable Flash Memory	Digital Cameras store digital photographs on removable SD Memory Cards. A standard 2GB SD Card can hold up to 380 images. Without investigating each individual camera and its associated memory card, there is no way of knowing how sensitive the information is that is stored on this device. Some older, and almost all current, medium to high spec cameras now have GPS location abilities for every photo taken and Wi-Fi connectivity. Again this information can be interrogated and opens your network to potential attack. This means the whole device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Camera has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Camera disposed of. Follow Control Process 1 & 3 & 4 & 5 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
10. USB memory sticks/Flash Drives	Flash Memory	Currently USB memory sticks can have a storage capacity of up to 1TB. As an organisation when disposing of USB memory sticks, you will have no way of knowing without inspecting every single USB stick, what information is stored on this media, if it has been encrypted, or how sensitive it is. We do know that North East Lincolnshire Council was fined £84,000 when they lost a memory stick containing data relating to around 286 pupils aged between five and 16. The costs of compensation, lost faith notifications and rectification actions will push this breach in to the £millions. This means each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every single item of Flash Memory has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every single item of Flash Memory disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
11. Mobile Phones	Internal Flash Memory and Removable Flash Memory	Today's mobile telephones are mini computers. They can store 64gb of information. There is freely available software that can be downloaded from the internet that when plugged into a phone will strip all data and categorise you contacts, there details and email addresses, the conversations you have had with each contact and what images you have stored. It will also categorise all bank account and financial information held on the device and place it in a searchable database. Mobile phones are dynamite for the information they now hold. In Nigeria reused mobile phones values are not based on how new or what model they are, but on the amount of personal data they hold. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Mobile Phone has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Mobile Phone disposed of. Follow Control Process 1 & 3 & 4 & 5 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
12. Tablets	Internal Solid State Drive Possible Removable Flash Memory	As technology progresses more and more wireless devices are used within organisations. There are now also BYOD (Bring Your Own Device) schemes being implemented and tablets constitute a large amount of these devices. Tablets use SSD's (Solid State HDD's) and these are digital. All the data is stored on a device that home users can access if required. To restore a device to "factory Settings" would not delete any company data transmitted via that device. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Tablet has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Tablet disposed of: Follow Control Process 2 & 3 & 4 & 6 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
13. EPOS Systems	Internal Hard Drive Possible removable Flash Memory	EPOS systems, Standalone till units, all use data storage to “remember” the software package they use. This may be in the form of a SSD a Hard Drive, or a CF card. Although this data may not mean much to most people, it can be accessed using minimal effort. This can uncover private external IP addresses, “friendly” URL’s for ease of access and also show potential routing information. Dependant on the Epos System, more serious threats such as customer information and purchase information may also be stored. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every EPOS System has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every EPOS System disposed of: Follow Control Process 1 & 3 & 4 & 6 & 7 & 8 & 9 & 10	High	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
14. Dictaphones	Magnetic Data Storage Tape	Not all data, is kept in a "digital" format. Recorded voice conversations can also pose a huge security threat and as Dictaphones become digital and have built in storage, although you click delete after using what was required, has it really been deleted? Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Dictaphone has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Dictaphone disposed of. Follow Control Process 1 & 3 & 4 & 5 & 8 & 9 & 10	High	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
15. Video Tapes	Magnetic Data Storage Tape	Video tapes are not only used for “video” but can also be used as legacy data backups. Any images recorded on this type of media falls into the same pitfalls as CCTV data. It could breach numerous Data Protection Act byelaws. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Video Tape has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Video Tape disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
16. Back-up tapes	Magnetic Data Storage Tape	Server/computer backup tapes contain a full “image” of a server or hard drive for disaster recovery solutions. These can be accessed and the files viewed using any backup software. Encryption for these devices is not standard so they could be accessed by anyone. As it creates an image of a hard drive it contains all files and folders, private or non-private so all documents relating to customers, members of staff can be accessed. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Back-up Tape has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Back-up Tape disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
17. Floppy Discs	Magnetic Data Storage Tape	Although a potentially outdated technology, floppy disks were used as a major source of data backup and transferring. This includes potentially confidential information and maybe old customer records. Although maybe not relevant to a company now but could contain financially sensitive data. It is very rare that mainstream computers have floppy drives now but they are still available and people will investigate to see what information can be found. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Floppy Disc has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Floppy Disc disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	Medium	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
18. CD & DVD's	Optical Data Storage	CD-R/W and DVD-R/W are possibly one of the biggest threats of removable media for a business. Blank CD's are "burned" with data. Even on a re-writable CD/DVD the original data is still available for anybody with any purpose to try and interrogate. Many of these discs are created without labels or markings so nobody is aware of what data is contained on them. These could be SAGE backups or internal corporate data. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every CD-R/W and DVD-R/W has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every CD-R/W and DVD-R/W disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
19. Zip drives	Magnetic Data Storage Tape	Iomega Zip Drives were medium-capacity “super floppy” drives and could hold up to 750mb of data. Although this does not seem a great deal, if they were used as a device backup, or even transferring data from one site to another they could hold sensitive Information and the drives to access these devices are very common. There is minimal encryption and as they were re-writable you could never be sure of what data has been left on them. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Zip drive has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Zip Drive disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	Medium	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
20. HDD's	Hard Disk Drive	As technology advances, so does the storage capabilities of a standard desktop PC. Modern HDD's now average approx. 512GB of data. On a company PC, this is all classed as company data and there are a variety of different software packages to interrogate and "view" the data. There is a huge misconception of formatting and erasing a HDD. Formatting simply writes to the first sector of a hard drive to allocate a file system. Meaning if you format a HDD it is still full of the data previously there, it is simply hidden from the current operating system. All the previous data is retrievable if required. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Hard Drive has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Hard Drive disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	Extreme	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Data Storage Device being assessed?	What are the Risks?	Degree of Potential Harm?	Process to either eliminate or reduce the of a Data Breach happening	Probability of a breach if process not followed	Probability of a breach when process is followed	Risk Rating
21. Solid State Hard Drives	Solid State Drive	Solid state HDD's are the latest variant of PC data storage, no moving parts, exceptionally faster than a standard HDD and very affordable. Formatting one of these devices, again like a standard HDD, only rewrites one sector of information for use by an operating system to view the data. Any data not overwritten, simply "deleted" is available for anybody with any intent to find and compromise. Each individual device should be categorised as highly sensitive with the probability of causing a severe data breach should it not be dispossessed of correctly.	With the average cost in 2017 to UK based Organiations for a single Data Breach being £2,480,000 , correct audited methods of data destruction that provide undeniable definitve proof that the data every Solid State Drive has been destroyed needs to be obtained. The following Processes ensure 0% risk is achieved for every Solid State Drive disposed of. Follow Control Process 2 & 3 & 4 & 5 & 8 & 9 & 10	High	Zero	Low Risk

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Control Process Number	Data Storage Device Types	Additional precautions needed to eliminate or reduce the hazard to at least a Low risk or ideally a Zero risk	Who is responsible for implementing these controls?	When controls to be implemented
1	No's 1 & 2 & 3 & 4 & 5 & 9 & 11 & 12 & 13 & 14	A Record of the serial number make and model of all equipment should be recorded before uplift by the Data Controller and catalogued in an Asset Management System. This enables the Data Controller to cross reference the equipment collected with the Asset Report provided by the Data Processor after completion of the collection. Notification of any additional items should be given to the Data Processor prior to uplift as the Data Processor will only be able to take listed items. The equipment should be stored in a secure location where no unauthorised access is permissible. Where possible the equipment should be factory reset.	Client/ Data Controller	Before Uplift
2	No's 6 & 7 & 8 & 10 & 15 & 16 & 17 & 18 & 19 & 20 & 21	A Record of the serial number make and model of the equipment should be recorded before uplift by the Data Controller and catalogued in an Asset Management System. This enables the Data Controller to cross reference the equipment collected with the Asset Report provided by the Data Processor after completion of the collection. Notification of any additional items should be given to the Data Processor prior to uplift as the Data Processor will only be able to take listed items. The equipment should be stored in a secure location where no unauthorised access is permissible. At this point the Data Controller will identify how many data storage boxes are required and confirm this with the Data Processor. Data Controller must place data storage devices securely in the GPS tracked data storage box and secure with signed cable ties before collection.	Client/ Data Controller / Data Processor	Before Uplift
3	No's 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21	A CRB Checked Driver will arrive onsite in a GPS tracked vehicle. Driver will tag items, count and verify with the data controller, a counter signature will be obtained and any additional items that have not been declared will not be taken. Any data security box or boxes that hold data bearing devices will be given to the driver where the GPS tracking will commence once the driver has left the Data Controllers site. A countersigned waste transfer note and collection note will be given to the data controller identifying the chain of custody .	Data Processor/ Data Controller	During Uplift

TELEPHONE: 01244 289 023

EMAIL: office@ecosystems-group.co.uk WEB: www.ecosystems-group.co.uk

Data Storage Device Risk Assessment & Method Statement

Control Process Number	Data Storage Device Types	Additional precautions needed to eliminate or reduce the hazard to at least a Low risk or ideally a Zero risk	Who is responsible for implementing these controls?	When controls to be implemented
4	No's 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21	On arrival at the Data Processors secure premises the GPS Tracked Vehicle will notify reception he has arrived and he will be met at the site entrance by the Logistics Manager. All equipment will be checked and verified against countersigned paperwork. This process is video recorded at all times. All equipment is placed in an assigned processing bay and all data storage boxes are immediately removed to a secure processing area with restricted access that can only be entered using a radio frequency card to authorised persons, again this area is fully covered by CCTV operation which is recorded and can be reviewed at any time. Once the vehicle is emptied it is again checked by the Logistics Manager before leaving the premises. Cab area's are also checked and all drivers must leave the Data Processors site through our Airport Style body security Scanner. The facility has one entrance/exit for vehicles via Enclosed 12 foot high Electric fencing and a roller shutter door that is closed except for inbound deliveries and covered by CCTV. All secure areas within the facility are only accessible via Radio Frequency Cards with limited access.	Data Processor	Before Processing
5	No's 3 & 4 & 9 & 10 & 11 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21	All GPS tracked Data Boxes are taken directly to the secure Data Erasure and Destruction Area for processing. The items stored in this box will have their serial numbers/asset tags recorded then destroyed using a shredder, this process will be supported by individual certificates of destruction evidence will be available on the asset report.	Data Processor	During Process
6	No's 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 12 & 13	All items situated in the secure designated bay area are separated between data bearing items and non data bearing items. All Data Bearing items are set to the secure data destruction For non-data bearing items all types, makes models, weight, C02 offset, serial numbers and asset tags are recorded on to the asset report. When agreed with the client a basic box count only is supplied The data erase and destruction area is based on the first floor and requires card code entry and no unauthorised persons can gain access at any time, it is also has full CCTV monitoring.	Data Processor	During Process

Data Storage Device Risk Assessment & Method Statement

Control Process Number	Data Storage Device Types	Additional precautions needed to eliminate or reduce the hazard to at least a Low risk or ideally a Zero risk	Who is responsible for implementing these controls?	When controls to be implemented
7	No's 6 & 7 & 8	All Laptops, PC's and Servers are connected to our bespoke Ecokill system. The system runs a programme that records the Collection Job number and the asset tag of the equipment then automatically captures all pertinent information relating to this equipment such as serial number, make, model, with technical specifications such as CPU type, speed, installed Ram, installed HDD's, HDD serial numbers. Once the EcoKill programme has captured the technical information it runs a KillDisk data destruction programme on a British HMG IL5 baseline standard. On completion of the data destruction process a certificate of data destruction is generated by the system and uploaded to the asset report on the client portal. Equipment where the HDD fails the process have the HDD removed and manually scanned, the HDD is physically destroyed with an individual certificate of destruction uploaded to the asset report on the client portal. Equipment that is non-working has the information manually recorded and added to the asset report, with the HDD removed and placed in to the EcoKill standalone system. This programme captures the Collection Job Number and serial number, then associates it to the equipment it was removed from then runs a data destruction programme on a British MHG IL5 baseline standard. On completion of the data destruction process a certificate of data destruction is generated by the system and uploaded to the asset report on the client portal. Equipment where the HDD fails the process have the HDD removed and manually scanned, the HDD is physically destroyed with an individual certificate of destruction uploaded to the asset report on the client portal.	Data Processor	During Processing
8	1 & 2 & 3 & 4 & 5 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21	Any data bearing devices that do not hold a serial number or asset tag will be given a unique barcode and displayed on your asset report to give full track and traceability. They will then be shredded and when requested an individual certificate of destruction uploaded to the asset report giving you definitive proof of destruction.	Data Processor	During Process
9	No's 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21	A fully detailed asset report, Certificates of destruction and WEEE Certificate will be delivered within 2 weeks of the collection date showing you have been fully compliant under the WEEE Directive and EU DPR.	Data Processor	On Completion