



COUNTING THE COST OF HAVING YOUR DATA COMPROMISED WHEN AN EMPLOYEE LEAVES...

EX-EMPLOYEE DATA CAPTURE & FORENSIC ANALYSIS SERVICE

There is almost always the risk of compromising confidential information when an employee leaves either by your data being intentionally deleted, destroyed or passed on to a competitor.

TYPICAL SCENARIOS:-

1. An employee emails confidential information to your competitors or deletes confidential information before departing.
2. Transferring a computer to another employee only to find that sensitive data has been deleted, overwritten or leaked.
3. Needing to know what data was on an employees computer and what happened to that data after they had left.

WHY MAKE USE OF THIS SERVICE?:-

Having a bit-by-bit image of the data device made as soon as possible (before or after the employee leaves), captured in accordance with good forensic practices, by a 3rd party, kept in a safe environment, for a set period of time, and preferably having all confidential data removed from the original device, prior to re-using it, will place you in the best possible position to:

1. Perform an investigation should it be required in the future.
2. Minimise leakage of your information, now, or in the future by the next user.
3. Avoid possible non-compliance due to data retention legislation.



WHAT ARE THE STEPS? - YOU HAVE 3 BASIC OPTIONS TO CHOOSE FROM:-

Option 1 -

1. We receive the computer (PC, Laptop, PDA etc.) & make a bit-by-bit image of the drive or memory device.
2. We keep the image for 12 months, or longer should you require.
3. Return the original data device with or without removing the confidential information.

Option 2 -

1. We receive the computer (PC, Laptop, PDA etc.) & make a bit-by-bit image of the drive or memory device.
2. We keep the image for 12 months, or longer should you require.
3. Perform a complete data recovery.
4. Return the original data device with or without removing the confidential information as well as the recovered data.

Option 3 -

1. We receive the computer (PC, Laptop, PDA etc.) & make a bit-by-bit image of the drive or memory device.
2. We keep the image for 12 months or longer should you require.
3. Perform a complete data forensic investigation.
4. Return the original data device with or without removing the confidential information, including a forensic report of our findings, as well as the recovered data.

FREQUENTLY ASKED QUESTIONS:-

Q1 - Can we at a later stage decide to continue with a full forensic investigation?

A - Yes, you can at any time continue with a full forensic investigation as long as the original image is still in our care.

Q2 - Can you keep the original image for longer than a year?

A - Yes, we can on request, although there is a cost implication.

Q3 - Why do you keep the data image?

A - It is advisable to keep the image in a safe environment at our premises (a 3rd party) in order to maintain good forensic practices.

Q4 - How long will this take?

A - The image normally takes 1 day. The forensic investigation can take as long as 14 working days depending on the complexity of the situation.

Q5 - What is the difference between a data recovery and a forensic investigation?

A - A forensic investigation includes all the processes involved with a data recovery plus an analyses of all the data on the drive drawing up a report on our findings.

DEFINITIONS:-

Bit-by-bit image - An exact Bit level, operating system independent, copy or clone of all available sectors, including hidden or system sectors from an electronic data device.

Bit - or binary digit - The smallest unit of information on a machine - either a 1 or a 0.

Confidential information - Sensitive or valuable information relating to the your strategic objectives & planning for both your existing & future needs, your business activities, relationships, products, services, customers & clients, demonstrations, processes & machinery, plans, designs, drawings, functional & technical requirements & specifications; information contained in your software & associated material documentation, technical, scientific, commercial, financial & market information, know-how & trade secrets; information concerning faults or defects in your systems, hardware &/or software or the incidence of such faults or defects...

Data device - A device capable of storing electronic data for future use i.e. hard disk drive, Solid state disk, memory stick or compact flash, CD/DVD, tape, M.O. disk etc.

Forensic investigation/analysis - Typically determining, extracting (recovering) and reporting from an electronic data device:-

- What files and other data were deleted and when (i.e. documents, emails, databases etc.)
- When last was the computer and files accessed.
- Where, when and from whom were emails sent and received.
- What emails were deleted and when.
- What programs that were deleted or uninstalled and when.
- What websites were visited and when.
- Files and other data protected by a password, encryption, compression or other methods.

With or without removing the confidential information - We can permanently erase any existing data (documents, emails etc.) without damaging the operating system or other program files.

We specialize in the recovery, protection, safekeeping, storing, retrieving, converting, investigating, unlocking and even destroying of your digital information, from server and RAID volumes, PC and laptop hard disk drives, backup tapes, CD & DVD media, non-volatile memory devices, MO media, stiffy diskettes and almost all other types of digital data media, irrespective of the condition of the media, including electro-mechanical failure, data corruption, virus infections, data deletion, or any other potential data threatening situation.

Please do not hesitate in contacting us should you require more information.

HELPING YOU LOOK AFTER YOUR DATA

Tel (S.A.) : 0860-600-800
Tel (Int.) : +27 (0)12-665-2945
Fax : +27 (0)12-665-4928
Mobile : +27 (0)82-600-5031
email: : sales@datarecovery.co.za

20 Uitzicht Office Park
5 Bellingham Street
Centurion
South Africa
0046