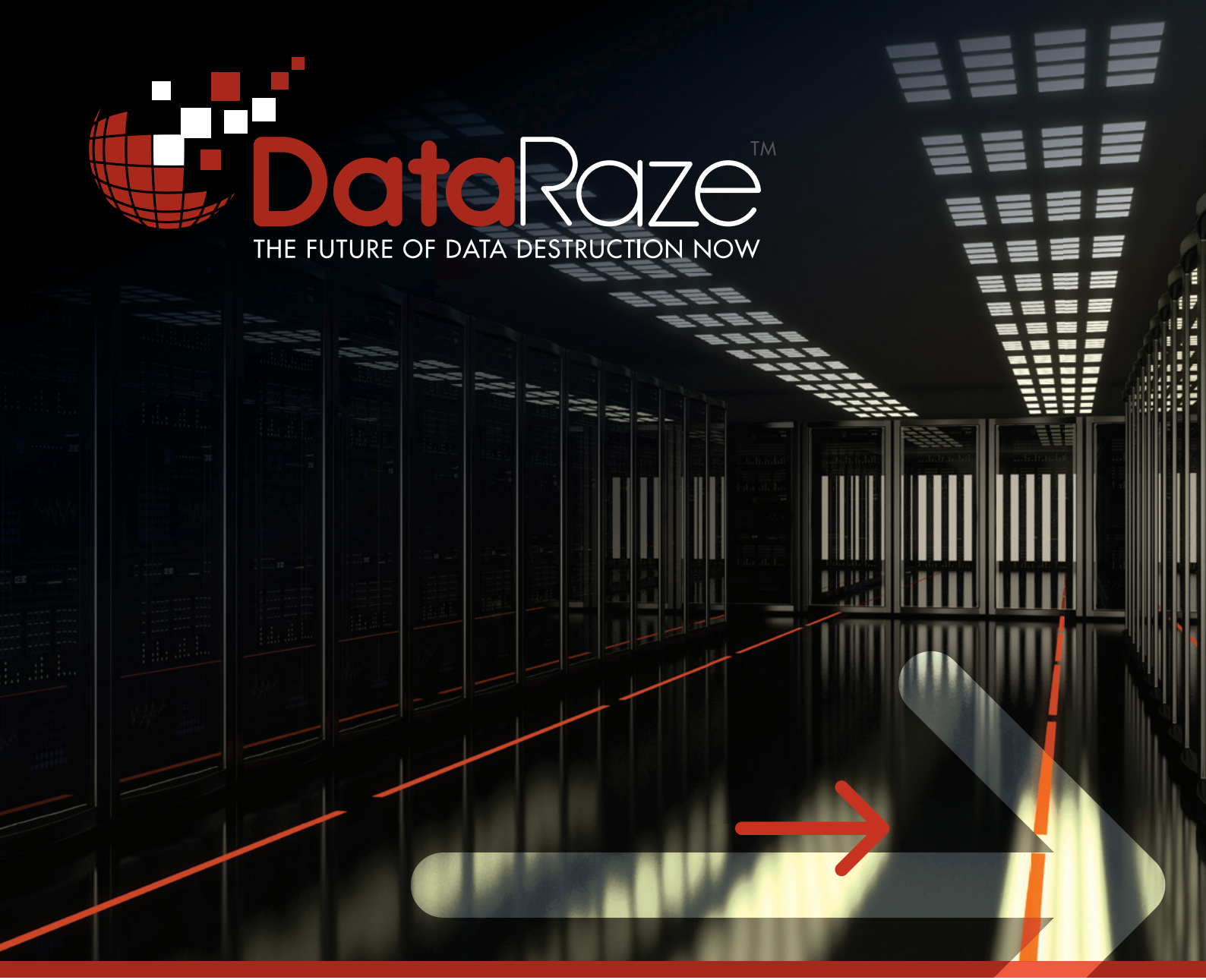

DataRaze™
THE FUTURE OF DATA DESTRUCTION NOW

THE FUTURE OF DATA DESTRUCTION IS NOW...

DataRaze has been developed to overcome and eradicate incidences of data breach by placing secure auditable, data protection and destruction practices in the hands of corporate IT Professionals.

Almost 100% of data breaches occur due to weak and ineffective internal processes. Company practice, security and compliance continue to demand greater scrutiny and evidence of data destruction, driven by stakeholders and shareholders alike. Data theft is reported almost daily, with organisations, both public and private, forced to find a futureproof answer.

As the cloud and outsourcing of IT managed services becomes preferred practice, data and asset management controls are crucial to protect businesses and individuals' privacy. Most think they have it 'wrapped up' – but they haven't!

What **DataRaze** brings to the market is a secure, auditable and user managed solution to enforce control of assets holding critical data and confidential information.

Data Controllers have never before had the opportunity to comprehensively monitor, police and report occurrences of data destruction before **DataRaze**.

– because it needs to be.

For too long, weak processes have been allowed to develop within organisations of all sizes, only to present themselves as embarrassing headlines over data breaches. Such data breaches and exposure of poor practice, will only increase if insecure 'chains of custody' are allowed to continue.

Current Options To **Erase Confidential Data**

1

Data Overwriting.
Methods and external supply for asset and data management services are well known and effective. Data overwriting is often the preferred method for removal of data. However on occasion, hidden, locked or damaged data may not be erased completely.

2

Degaussing.
Degaussing is another way of destroying data by passing a magnetic field through the drive, rendering it unusable. However, degaussing may prove ineffective if the drive is heavily shielded.

3

On-Site Hard Drive Shredding.
Increasingly, hard drive destruction is seen as the ultimate solution to destroy both data and the media storing it. However, this method does not provide evidence of the life cycle of the media and is therefore not auditable.

All of the above solutions, provided as an external service, to erase or destroy the data, are effective. However without evidence of an audited or secure chain of custody there is no verification that the task has been carried out to satisfy constant enquiries from internal data security and compliance auditors.

SO WHO ARE DATARAZE?

Some organisations are satisfied to store hard drives until a sufficient number are gathered, then arrange for an on-site service to shred multiple hard drives. The current method used, only records the serial number of the device before the operator places the drive into the shredding machine. Machines can destroy hundreds of drives per day, so for bulk destruction of low impact level data, this will suffice….

DataRaze has taken a monumental leap forward to offer and deliver real time auditable data and asset management 'controlled in-house', on a schedule suitable to the organisation. A 'chain of custody' breach during the time elapsing between the removal and storage of the drive and its eventual destruction, is when authorisation, control and responsibility are at their most critical.

DataRaze has been developed to eradicate the flaws with existing internal processes, where data passes along a potentially insecure chain of custody route. It is imperative to safely deliver data bearing media for destruction using as few steps as possible.

DataRaze has taken technology and created a long awaited futureproof secure solution. Secure access to **DataRaze** via biometric technology ensures only authorised members of the team use the system. Details of the asset, including the department that owned and created the data, will be recorded and reported.

DataRaze allows you to destroy your data when it's critical for you, recording these actions with digital and video evidence, reporting each destruction occurrence. All evidence of the shred destruction process is recorded.

ORGANISATIONAL SECURITY

Organisational data security is not about one department or a local office or relying on one member of staff, it's about protecting the whole organisation wherever they are located.

Remote Web Access to the **DataRaze** system ensures that those needing to know that a defective drive has been removed are kept informed, indicating when this occurred and who was responsible. These practices must form part of your internal process to clearly map such events. A 'cradle to grave' procedure can be achieved if staff utilise the auditing capabilities of **DataRaze** to provide much improved security throughout the organisation.

As part of its process, **DataRaze** will request an expected date of arrival for the drive intended for destruction. Each time a drive is returned to **DataRaze** a report will alert the Data Controller that the drive has been returned and registered. It will continue to alert the Data Controller of any drives that remain outstanding within the expected date/ period for destruction.

If the date of arrival overruns, then **DataRaze** would immediately alert the Data Controller that a drive holding data has not been returned or registered as expected, and remains on the "missing" list recorded on the **DataRaze** system.

FEATURES ARE:

- Fully computerised control of data destruction from start to finish
- User controlled software via touchscreen interface throughout, in a format of your choice
- Biometric user control with security authentication
- Multiple levels of users individually identified via bio-metrics
- Camera identifies user whilst system is in use to prevent crossover of non-secure staff
- Manual input to identify the media source and authorisation for destruction
- Secure non-returnable media housing, with digital authentication and marking of original media serial number
- Senior level and matching authorisation needed to release hatch for drive retrieval
- Shredding mechanism is securely concealed inside the unit with access only to engineering level personnel
- 3 second video capture when media is being destroyed contained on reports
- User Interface takes the user through each step from entry to final shredding process and sign off
- Data-controller can access and personalise reports to suit organisations requirements
- Waste Transfer Notes are produced and stored to be printed when needed
- Web Interface access for easy administration and function

KEY FEATURES AT A GLANCE

QUIET AND QUICK OPERATION →

FULL LIFECYLE AUDIT TRAIL →

PRODUCT SPECIFICATIONS

- All components and DataRaze systems are electronically tested and CE approved
- Standard version runs on 240VAC/13Amp (single phase version)
- Heavy duty version will run on 415VAC/16Amp (three phase version)
- Shredder internals protected by safety interlocks
- Shredding chamber double-shielded and fitted with safety interlocks
- Interlock 'trip' will result in automatic shut-down for safety purposes
- Emergency stop switch fitted externally
- Low noise and unit insulation
- Flush fitting components to avoid protrusions
- Adjustable face camera height for different users
- Built in RCD's (Residual Current Device)
- Overload and overheat protection built in
- No direct access to shredding chamber at any time

TOUCHSCREEN INTERFACE

BIOMETRIC OPERATOR ACCESS

WHAT IS DATARAZE...

DATARAZE IS A 'SECURE USER CONTROLLED MEDIA SHREDDER'.

HOW DOES A USER GAIN ACCESS TO THE SYSTEM?

- Your organisation determines who should be granted access to use the system and sets their access level
- All of the users' actions are monitored and logged by the DataRaze system
- They are 'enrolled' on the system via biometric registration
- Their full user information is logged by the system as well as date, time, department and authorisation code. i.e., John Smith IT2695 (administrator)
- If not recognised as authorised by the system, login will not be allowed and a record of the access failure is recorded

HOW IS DATARAZE USER ACCESS CONTROLLED?

- The biometric enrolment ensures that each user is identified using unique credentials
- If recognised by the system, the screen displays a 'Welcome' message and allows them to continue at their level of authorisation
- The user can control the complete destruction process from start to finish with the right level of authorisation
- The system will log the user off after a set period of inactivity, preset by the Data Controller
- All allowed and denied access attempts are logged

...AND WHAT DOES IT DO?

This allows the Administrator to monitor access and investigate repeated login failures

- Reports are generated to assess what has been destroyed, by whom, from which business area, and why. These reports are accessible from a central console using any internet-capable device

- The system gives a complete audit trail for compliance and security purposes

HOW MANY USERS WILL THE SYSTEM ACCEPT?

- As long as the staff member has been set up on the system as an authorised user there is no limit. However, in the interests of security and management control, it is sensible to limit the number.

It is also important to remove those who no longer have authorisation

WHAT OTHER INBUILT SECURITY FEATURES DOES DATARAZE HAVE?

- Every time the user prompts the machine to destroy a hard drive, an in built camera takes an image of the user. This is transmitted as a digital image to the system database for audit and security purposes

WHAT STEPS TAKE PLACE PRIOR TO SHREDDING?

- Every time the operator wishes to destroy an item, after signing in, the system will ask for information to verify the media and its source (the serial number of the hard drive, department it originated from, who authorised the

Q&A (CONT.)

shredding, the asset or serial number of the PC it came from, etc). These information fields can be customised as required by the client. For the serial number entry to be recorded, a hand-held scanner is included to make this step more efficient and avoid human error

WHAT HAPPENS NEXT AND HOW DO WE AVOID MEDIA IDENTIFICATION ISSUES?

- Once the details have been entered as above, a recessed tray compartment will open to allow the media to be locked into the DataRaze
- The media is then taken into the system. From this point on it cannot be removed by the user currently authorised to activate the DataRaze
- An in-built imaging device then scans an image of the manufacturers serial number label attached to the media
- The system then compares the recorded serial number of the media with the serial number scanned earlier by the user
- If the media label image and the data entered by the user match, then the user will be prompted again to proceed with the shredding. This action is displayed on the touch screen and recorded
- If the user decides not to proceed at this point, then a message will be sent to the administrator requesting they attend the unit and investigate the issue
- Only when the administrator logs in to the system will the media hatch open to release the device. At this point the administrator can authorise the destruction of the media to continue
- The original user will then have to re-register his or her log in to commence the process again

WHAT HAPPENS AFTER SUCCESSFUL DESTRUCTION OF THE MEDIA?

- Each time shredding of a device has been completed, a prompt appears on the

screen asking the user if they wish to continue

- If the user decides NOT to destroy any more devices during this logged in session, then a prompt appears to ask the user to exit the system
- The system will automatically close down regardless, after a pre-designated period
- If the user forgets to log out of the system then the session will automatically end, returning to the login screen
- A complete record of the successful or unsuccessful destruction is logged by the system and available immediately for viewing by the administrator
- The administrator or other authorised users can view details about the shredding completed including the image and details of the media and operator
- User-defined reports can be generated using the in-built database display and exported as required, to internally interrogate the data

HOW WOULD WE ARRANGE FOR COLLECTION OF SHREDDED WASTE MATERIALS?

- The DataRaze unit has a built-in electronic weighing mechanism. It will be set to alert DataRaze support when it reaches capacity
- With the client's permission an automatic email alert will be sent to the central DataRaze Support team and a support engineer will be despatched
- Collections can be arranged directly if preferred

Q&A (CONT.)

WHAT DO WE RECEIVE WHEN THE WASTE MATERIAL IS COLLECTED?

- A DataRaze support engineer will attend your site and activate the system with their own biometric details
- The waste material will be emptied into a lockable bin and removed from site
- A Waste Transfer note will be produced and signed, for all waste collected
- The system can produce a printed report of all waste removed by date, weight or period

HOW MUCH MEDIA CAN DATARAZE SHRED BEFORE IT NEEDS EMPTYING?

- This depends on the media type destroyed but on average around 100-200 media items (3.5" hard drives) depending on weight and density
- The DataRaze system and support team will handle all waste measurement and collection requirements

WE MAY WANT TO SHARE A UNIT BETWEEN DEPARTMENTS, CAN WE DO THIS?

- Whilst this is possible as the unit is portable, we would advise the media be taken to the unit. Never forget the security implications with distributing such a device. You will need to limit the number of staff with biometric access too and we strongly recommend you keep the number low to maintain security at the highest possible level internally

DOES DATARAZE CONTAIN MOVING PARTS?

- All moving parts are concealed beneath the casing of DataRaze and

are not accessible to the user. Only a DataRaze support engineer will have access to internal parts and mechanical functions

HOW NOISY IS DATARAZE AND COULD WE HAVE IT IN AN OFFICE AREA?

- DataRaze is insulated and lined with acoustic materials to prevent unnecessary noise levels.
  We would recommend deployment to your organisation's IT area

WHAT SIZE OF SHREDDED MATERIAL DOES DATARAZE PRODUCE?

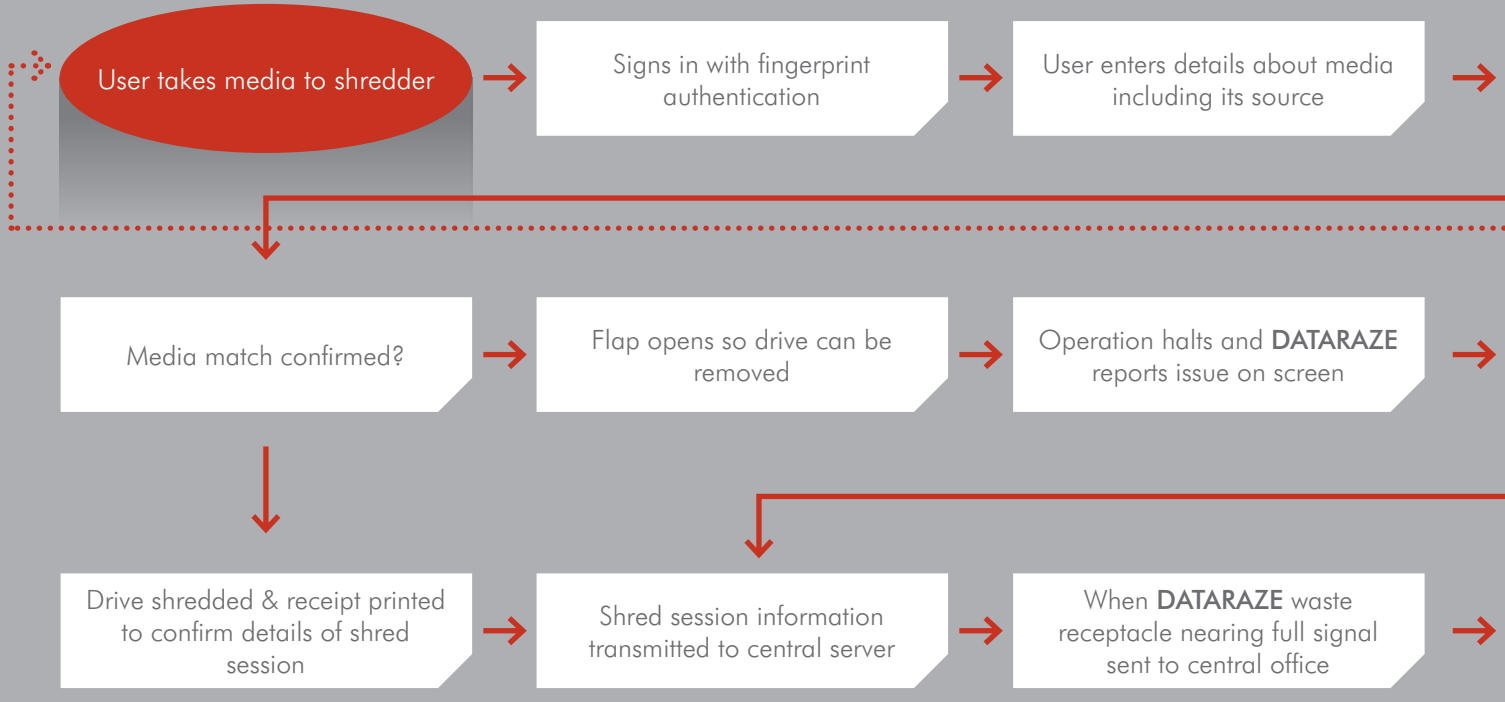
- DataRaze meets the industry standard for particle size which is 15-30mm.

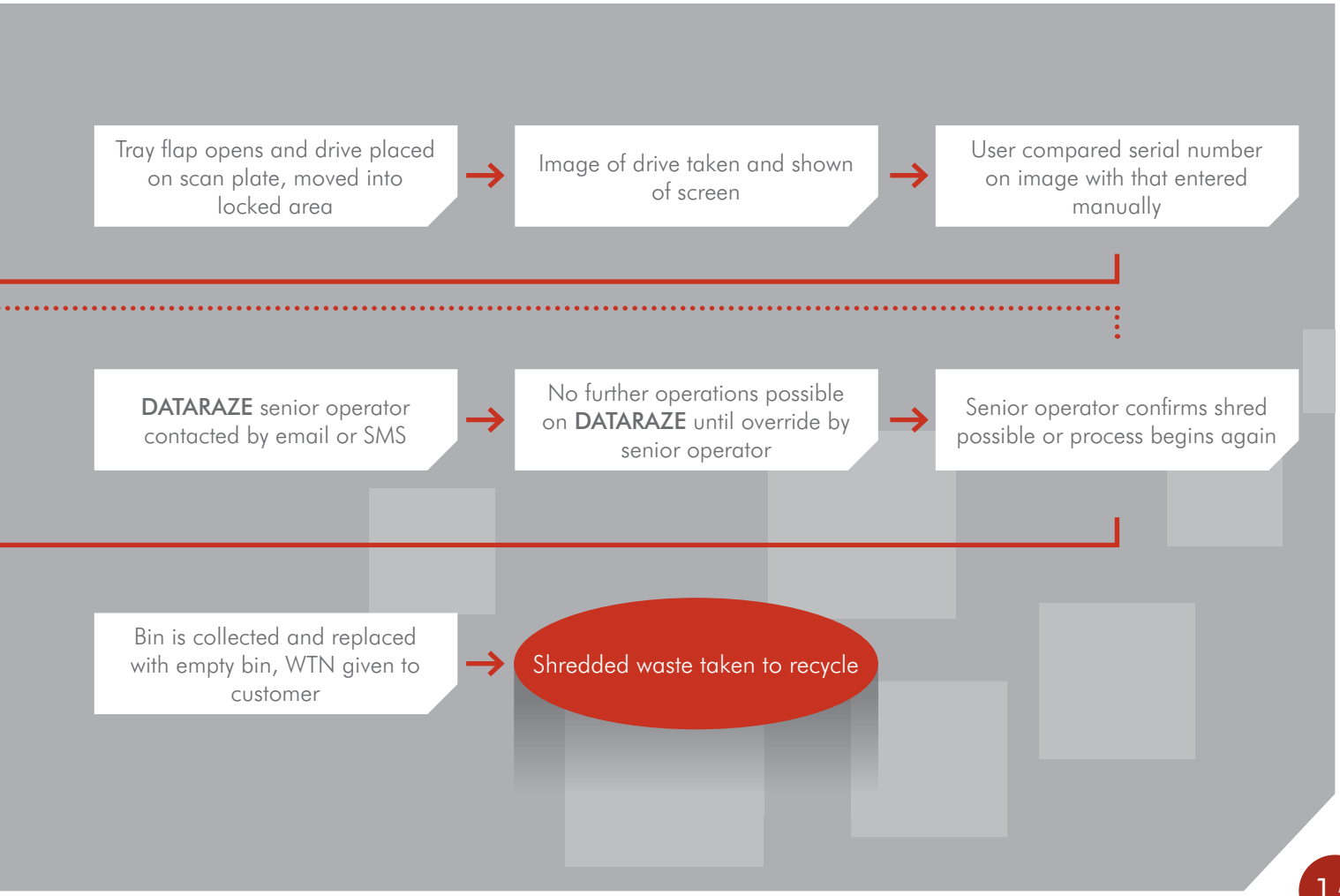
The size of shredded material is determined by the internal mechanism of DataRaze but driven by an organisations security policy. Data held falls into Impact Level Categories known as IL4, IL5 or IL6. The coding determines the internal security levels of the data

WHAT HAPPENS TO THE WASTE MATERIAL?

- DataRaze uses Environment Agency approved refiners to dispose of the mixed metals and plastic waste created responsibly. DataRaze carries out its own audits to ensure our partners adhere to our policies and procedures

DATARAZE PROCESS




Tray flap opens and drive placed on scan plate, moved into locked area
Image of drive taken and shown of screen
User compared serial number on image with that entered manually
DATARAZE senior operator contacted by email or SMS
No further operations possible on DATARAZE until override by senior operator
Senior operator confirms shred possible or process begins again
Bin is collected and replaced with empty bin, WTN given to customer
Shredded waste taken to recycle

www.dataraze.co.uk

E. info@dataraze.co.uk