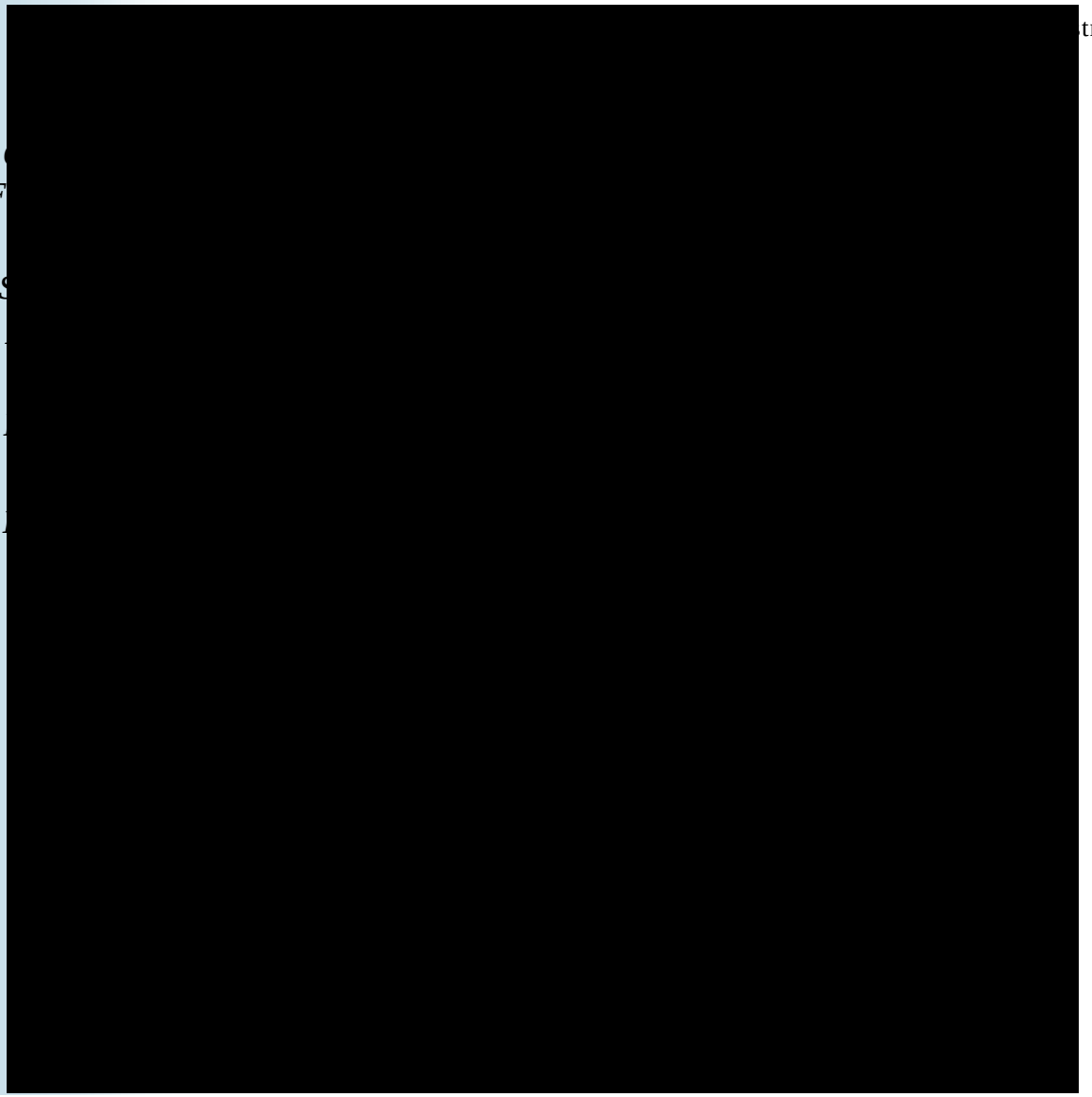
"Safety Comes First"

Case Western Reserve Environmental Health and Safety



trings. While

"The 'Shut the Sash' initiative at CWRU is valuable for

Make sure that the

"Promptly report any hood that is not functioning properly to your supervisor and EHS (368-2907)."

Surveying Radioactive Packages

"Once the laboratory receives it's package, they must open and survey the package the SAME day that it arrives."

Before any radioisotopes can be delivered, they are first screened by the Radiation Safety Office. The outside of the package is checked for contamination to ensure that it can be safely handled and delivered to the laboratories and the Packing Slip is checked to ensure that the proper item ordered was shipped out. The Packing Slip, Package Receipt Form, and Purchasing Form are all attached to the top of the radioactive material containing package. The package may not be delivered without this paperwork attached.

Once the package reaches the laboratory, it must be opened and surveyed the SAME day it arrives. Both a wipe test and a meter survey should be performed and recorded on the Package Receipt Form that was attached to the top of the box by Radiation Safety. There is space on the form to record your survey results. The liquid scintillation counter print out must have the date and time of analysis on it and should be attached to this form by the laboratory. If the package contains a high energy beta emitter such as P32, Cl36, or Na22, the wipe may be checked with a Geiger counter rather than running it on a scintillation counter. These surveys should be kept in the laboratory's radiation notebook and be available for inspection by the Radiation Safety Office.

If no contamination is found, the laboratory may deface and dispose of the box and

Introduction to Data Security

Data security is ensuring that unauthorized persons cannot access data, while ensuring that authorized persons can access data which is identical to the original. This can consist of several parts:

Redundancy: Avoiding data loss to random hardware failure.
Backup: Avoiding data loss due to localized failure.
Encryption: Preventing unauthorized reading of files.
Tamperproofing: Preventing unauthorized modification of files.

Redundancy consists of using several devices which can be used to take over for each other. The simplest form of electronic data redundancy is mirrored hard drives: both keep the same information, and if one fails it can be replaced; once it is replaced and the data replicated, the data is secure even if the second drive fails.

More sophisticated forms of redundancy exists. RAID level 5 allows for an array of any number of drives with only one redundant drives. If any single drive fails, no data is lost (though all data is lost if a second fails before the first is replaced and replicated). RAID level 6 allows arrays of any size with two redundant drives. This is not the same as mirrored (RAID 1+0) drives, even for the case of four drives where both have two redundant drives. RAID 6 can tolerate the loss of any two drives, while RAID 1+0 can fail if two paired drives are lost (though it can sustain the loss of two unpaired drives).

Offsite backup, on the other hand, protects against non-independent failures. For example, a flood or power surge might destroy all drives on an array; keeping a copy of the data elsewhere helps protect against these cases. Online backups are convenient but sometimes impractical for large amounts of data (though some services will ship drives with backup-up data for a fee, somewhat mitigating the disadvantage).

Encryption prevents people without the key from reading the data. Strong crypto is easily available which cannot be broken unless

“Offsite backup, on the other hand, protects against non-independent failures.”

Radioactive Packages, Cont.

There are disadvantages, though: if the key is lost then the data cannot be restored. Similarly, if there is damage to the physical media containing encrypted data it usually cannot be restored, even with the key, so encryption

"…. encryption should rarely be used without redundancy or at least backup."

The containers must be dated when removed from [illegible] accumulation areas (labs) and sent to the central chemical waste storage facilities.

For further information on container storage issues and solution, feel free to contact Environmental Health and Safety at 368-2906.

Source: The BLR Environmental Daily Advisor, August 21, 2012.

EHS STAFF

Victoria COOK (vcook), Health Physics Specialist II
Gwendolyn COX-JOHNSON (gwendolyn.cox-johnson), Department Assistant II
Jim DAHLE (james.dahle), Fire & Life Safety Specialist I
Bill DEPETRO (william.depetro), Safety Services Specialist II
Anna DUBNISHEVA (anna.dubnisheva), Safety Services Specialist II
Charles GREATHOUSE (charles.greathouse), Analyst Programmer II
Kumudu KULASEKERE (kumudu), Health Physics Specialist I
Robert LATSCH (robert.latsch), Safety Services Specialist II
Jason MAY (jason.may), Chemical Safety Department Assistant II
Tom L. MERK (tom.merk), Assistant Director of Safety Services, ABSO
Yelena NEYMAN (yelena.neyman), Health Physics Specialist II
Joe NIKSTENAS (joenik), Operations Manager Specialist II, RRPT
Heidi PAGE (heidi.page), BSO, Safety Services Specialist II
Marc RUBIN (marc.rubin), Director of Safety Services, ABSO, CSO, ARO
Zach SCHWEIKART (zachary.schweikart), Industrial Hygiene Specialist II
Dr. Mary Ellen SCOTT (maryellen.scott), Safety Services Specialist II
Dr. W. David SEDWICK (w.sedwick), Director of Radiation Safety, Professor and RSO
Felice THORNTON-P

Please remember, all back issues of the EHS Newsletter can be found online at case.edu/ehs. Simply click on the "Newsletter" link in the left-hand column!