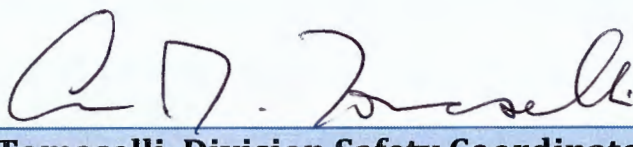
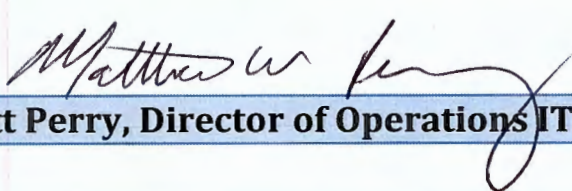


FY13 IT Division Safety Self-Assessment

Physical Access to IT Data Centers

X  7/12/13
Ann M. Tomaselli, Division Safety Coordinator

X  7/12/13
Matt Perry, Director of Operations IT

Physical Access to IT Data Centers

Submitted July 12, 2013

IT Data Centers manage critical systems at the Laboratory and need to be monitored and reviewed regularly to ensure the appropriate individuals have access to maintain these systems. The critical systems are housed in an area with a fire suppression system in place to protect the equipment that houses the data in the event of fire. Employees whose positions require them to access these data centers need to be aware of the hazards and proper response in the event of a triggering of the fire suppression system. Release of the suppression agent unnecessarily in the event of a smaller incident would be problematic.

This Safety Self-Assessment reviewed the process for obtaining access to the data centers and concludes that training is critical but could be streamlined, as well as a recommendation for a “light” (shorter) version of the training for 50A-2109. There is also an opportunity to connect the EHSS training database to the card key database to more automate the system and rely less on the annual review.

Finally, communication of IT access requirements with other divisions (Facilities and Protective Services) who need to help maintain the infrastructure for aforementioned systems, needs to improve to avoid inadvertently adding individuals to data center access lists without notifying IT.

1.0 Introduction

The IT Division reviewed access to one of its data centers as part of a 2010 Safety Self-assessment noting that “access needed further review”. This assessment is to address that review as well as expand it. Due to recent staffing changes it was appropriate to review the processes for managing access to IT data centers. Opportunities to link training to the current card keying system had also started to emerge at the Laboratory and it was considered that this might be an opportunity to initiate that link between systems.

2.0 Focus Area

Division Data Centers (50B-1275 and 50-1156) house the systems which support critical systems for LBLnet, Telephony, Cyber Security Operations , High Performance Computing (HPC) and Business Systems. These systems support both science and operations divisions including Human Resources, Payroll and EHSS. The physical access to these areas needs to be managed and reviewed to be clear that the appropriate individuals have access to the appropriate systems. The third data center, which is a co-located facility provided for various scientists who work for and with the Lab (50A-2109), does not have critical operations data nor does it have a Halon fire suppression system, so the access requirements are less strict.

3.0 Lines of Inquiry

The two main lines of inquiry for this exercise are 1) Do individuals who have access to IT data centers have a business need? And 2) Do individuals who have access to these spaces have the appropriate hazard training (EHS0361)?

4.0 Scope

In our Self-Assessment of this focus area we will ask in relation to IT's three data centers (50-1156, 50B-1275 and 50A-2109):

Are access lists updated and reviewed regularly?

Is IT working effectively with the Protective Services group and Facilities to administer access rights?

5.0 Methodology

- A. Person(s) conducting the self-assessment: IT Division Safety Coordinator (DSC), IT Data center manager, individual(s) updating card key access to data-centers, Protective Services Personnel responsible for card key access.
- B. Techniques to be used during the self-assessment.
 1. Review access lists
 - a. Request access lists for all IT card key controlled spaces
 - b. Identify authorizers for the spaces
 - c. Review access lists with authorizers
 - d. Identify any changes needed in access.

- e. Work with authorizers and inputters to make any necessary changes.
 - f. Formalize review process and document.
2. Access rights administration
 - a. Review access requests made through Protective Services
 - b. Confirm that CS is able to effectively back up IT Divisional inputter
 - c. Check that correct authorizers are used
 3. Badge reader function
 - a. Does badge reader link to training?
 - b. Does training link to JHA?
 - c. Test the system to see if identified issues have been resolved.
 4. Expiration notification effectiveness
 - a. Confirm staff receiving GERT expiration notification
 - b. Review email training expiration notification timeliness
 - c. Review email training expiration notification to assure it warns of access denial for GERT and EHS361 Computer Room Training.
 - d. Review JHA work groups and access lists to assure all staff who have access to computer rooms receive training expiration notification

6.0 Current Requirements

IT currently requires that those who are to access 50B-1275 and 50-1156, must have taken EHS0361 as well as have a verified business need. EHS0361 is supposed to be updated every three years though this is not a widely known part of the requirement.

50A-2109 which is a co-located facility where IT provides the infrastructure (power, network, coolant) for scientific divisions who wish to manage their own servers does not have the training requirement currently.

7.0 Assessment Results

Review of datacenter access found a process handled internally by the IT Data Center Manager who was the individual responsible for allowing access. This individual would also annually review the access to the space. There is no formal documentation of the process but a number of individuals, who would have concerns regarding the process, were aware of it being done annually.

Due to the recent retirement of the former Data Center Manager, there was an opportunity for the newly responsible individual(s) to help formalize the process.

In the past, the process has been that individuals needing access would contact the Data Center Manager who would then review and advise if the individual needing access a) had a business need and b) had taken EHS0361 computer room training. Once those two requirements were met, the Manager would advise the “inputter” to give the individual(s) access. The inputter had been an individual in Computing Sciences (CS) who had been the inputter for all card key access for IT. Since there was a growing need to review access, IT decided to make the Division Safety Coordinator the “inputter” for the IT division. The individual in CS would remain as back up as there had never been an issue with that individual so much as a concern from the IT division for greater understanding and control of the process for IT owned space.

One challenge was the grandfathering in of blanket access for certain groups who wouldn't necessarily need access. This included a group that comprised much of the Lab upper management (the COO, Lab Director, etc.) and security personnel. The blanket access issue was primarily related to 50-1156 since 50B-1275 seemed to be more regularly reviewed. After getting approval from the CIO and meeting with the owners of the program that manage card key access (Protective Services), it was determined that blanket access for upper management was not supported and would be turned off. Blanket access was also given to all in security, but subsequently given only to security personnel in supervisory positions. It was also agreed that those who should have access would have to take the training (EHS0361).

The following are gaps that were found with data center access that have been remedied:

1. The IT division did not have a designated “inputter” for cardkey access database. This role had been being fulfilled by the “inputter” from Computing Sciences. The Division Safety Coordinator volunteered to take on this role understanding that it was to “input” and create or delete access per the designated “approver”.
2. No formal process was documented. Upon completion of this Self-Assessment a process for how to gain access by the appropriate channels will be written, approved and posted on a yet to be determined website.

Observations

1. With the exception of GERT training, EHS361, which is required for access to IT's primary data centers (1275 and 1156), access is not automatic by just taking the online course. It is currently a manual process both to add and remove an individual or group access. There is software that can interface with the current system to rectify this. The software is available; it is an issue of obtaining the time and financing to correct the programming. (Improvement)
2. An individual who is not in a workgroup associated with EHS0361 training, but has in fact taken the training may be granted access. The training is currently supposed to expire after three years and be retaken. There is no current way to capture those who may have had a training lapse if they are not in the Datacenter work group. The way to manage those who currently have access, but are not in the work group, is to review annually. This requires the reviewer to ensure that those who have taken the training

have done so within the last three years. To do this the reviewer needs to look at the individual JHA or at the report for all those who have taken EHS0361 both found within the JHA system. Automation of this task would improve the robustness of the system. (Improvement and Line Management review.)

3. There is a disconnect between Facilities, Protective Services/Site Access and IT as to the requirements required to have access to the IT data centers. There was an incident where an individual from Facilities was given access to one of the data centers without the appropriate training or clearance from IT. The apparent reason the individual was given access was that when they began working at the Lab they were put into the system with the same settings as another employee. Unfortunately this was not realized for a few months (though this person never did access the data centers). (Corrective Action.)
4. Some staff do not receive reminders that their computer room training is about to expire, because they have not added themselves to the JHA computer room work groups. Responsibility for the accuracy of JHA's resides with the employee and the line manager. A manager may recognize this when reviewing staff JHA's and seeing EHS0361 as "recommended" instead of "required". The training is "required" if you are part of the IT Data Center workgroup and only "recommended" if you take it without subscribing to the work group. (Improvement and Line Management review)
5. Update EHS0361 to be more concise related to Halon hazard and Create an EHS0361 "light" for 2109 access. (Improvement)

8.0 Recommended Corrective Actions

Formalize process for requesting access including providing information across divisions. This is something we in IT need to do and communicate across divisions; specifically Protective Services and Facilities.

9.0 Suggested Improvements

1. Integrate EHSS training system to Site Access card key system so that process becomes automated. This is something that has to be done on the institutional level and not Divisional so we are unable to control this as a "Corrective Action" and instead suggest it as an "Improvement".
2. It could be useful to streamline EHS0361 and suggest a "light" version for 2109. IT will consider working with EHSS and Computing Sciences who have similar access requirements for data centers to review this.

3. There may be an opportunity to have those who currently have EHS0361 as “recommended” for training subscribed to the IT Data Center Workgroup so that the training will be “managed”. It will require some thought on how to implement this.

10.0 Conclusion

IT has managed their data centers on a risk based internal process that to date had not been documented. As a result of this assessment, that documentation will be remedied. For those items that are controllable within the division we have created Corrective Actions. For those items that require agreement with outside Divisions we have created Suggested Improvements. In both cases documentation and communication for processes surrounding access to technical areas, will require regular review, but hopefully can be more automated in the not too distant future.