**Computer Deconstructing Nanobot Procedure**

1. **Overview**

Physical protection of our data centers is essential to maintaining a quality experience for our users. Failing to protect against a potential Nanobot outbreak can lead to the devastation of the service that our data center strives to provide.

1. **Purpose**

The purpose of this document is to establish a procedure for dealing with Computer Deconstructing Nanobots.

1. **Scope**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

1. **Computer Deconstructing Nanobot Procedures**
   1. **General**

* Keep Calm, I’m the Doctor.
* Users will receive monthly training on Proton Packs.
* Users will be trained to ID Computer Deconstructing Nanobots.
* Users will also be trained on proper lock down procedures to contain the Nanobots.

**4.2 Standards**

**A.** Keeping the data center fully operational at all times is our top priority.

In the event of a Nanobot outbreak, the following should be done

1. Put on your Nanobot filtering mask
2. Isolate the data center immediately
3. Alert the Infosec team
4. Grab a Proton Pack
5. Use the Proton Pack to disable as many Nanobots as possible
6. DO NOT CROSS THE STREAMS!
7. Using the Proton Pack, ensure the perimeter is secure
8. Start a sweep of all computers
9. Wait for more help
10. **Enforcement**

Any employee found to be in violating of this policy will be “slimed”. The safety of our data center is in your hands! Do not fail the data center. Also, employees will face legal implications if they do not complete the procedure listed above adequately.

Works Cited

1. Web. 4 NOV. 2014.

https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

2. Web. 4 NOV. 2014.

http://www.uhd.edu/campus/handbook/documents/password\_procedure\_082410.pdf