**Computer Deconstructing Nanobot Policy**

**Free Use Disclaimer**: This policy was created entirely for fun and can be freely used by any organization. There is no prior approval necessary for use.

**Things to Consider:** Please take into consideration that nanobots, while real, do not pose a serious threat to our data centers.

**Last Update Status:** Created and Updated November 2014.

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 policy is to contain the damages caused by Computer Deconstructing Nanobots in the event of an outbreak.

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. **Policy**

4.1 Containment

4.1.1 Any user present during an outbreak will be expected to lock down the data center.

4.1.2 The User will activate the nearest Proton Pack stored at convenient intervals throughout the data center.

4.1.3 These Proton Packs are to be used to aid in the “Busting” of any Nanobots.

4.2 Proton Pack Storage

4.2.1 The Proton Packs will be stored throughout the building in order to maximize ease of access.

4.2.2 The Proton Pack will need to be function checked every 7 days, this will prevent any failures from occurring during an outbreak.

4.3 Proton Pack Training

4.3.1 It is the responsibility of the managers to ensure that all employees are trained on the Proton Pack

4.3.2 Whatever you do, DO NOT CROSS THE STREAMS!

1. **Policy Compliance**

5.1 Compliance Measurement

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

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1. **Related Standards, Policies, and Processes**

* Zombie Outbreak Response

1. **Definitions and Term**

* Computer Deconstructing Nanobot: Refers to a small robotic device that has been created for the sole purpose of deconstructing any computer it can locate. Deemed very dangerous to our technology infrastructure, the odds of ever seeing one of these is well beyond 1 out of infinity.

Works Cited

1. Web. 4 NOV. 2014.

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