Separation of Duties for Critical Functions in DCND (Production Account)

To prevent large-scale negative impacts from human error, hacking, or malicious intent, we are specifying a separation of duties for certain actions within OIT managed production accounts. This is a common method to help prevent foreseeable errors or malicious activity.

For the purposes of this document, we define **separation of duties** as the concept of having more than one person required to complete a particular task.

Currently, there are five specific areas where we would like to implement this policy:

1. Termination of production instances
2. Removal of production networking resources (VPCs, subnets, ACLs, VPC peering, Internet Gateways)
3. Modifications of production security groups
4. Access to the Root Account Password and MFA
5. Ability to change IAM access policies

Termination of Production Instances

- No user will be able to terminate EC2 instances with an Environment tag == 'production'.
- Only members of the Configuration Management team will be able to remove the 'production' tag, but they will not have the permissions to terminate instances.

Modification of Production Security Groups

- No user will be able to modify/delete security groups with an Environment tag == production.
- Only members of the Configuration Management team will be able to remove the 'production' tag, but they will not have the permissions to modify security groups.

Access to Root Account

- Access to the root accounts of all OIT managed production accounts will be separated.
- The virtualization team will control the password.
- InfoSec will possess the physical keyfob to supply an MFA token.

Ability to Change IAM Policies

- A service account will be created which will have the ability to create/edit/implement IAM access policies.
- Identity and Access Management will have the password to this account.
- InfoSec will hold the physical keyfob to supply an MFA token.
- InfoSec will continue to be responsible for defining university access standards while IAM will continue to responsible for implementing these standards in AWS. However, both parties will be required to be present to implement these policies in OIT managed production using the service account.
- For the duration of the CloudFirst program, someone from IAM and InfoSec should be available daily in ITC 114 to work on pending requests. After the program terminates, or when co-location is no longer the current practice, the two departments will set up regular meetings as necessary to process pending requests.

Mike Dunn, Kolin Hodgson, Jaime Preciado, Bob Winding

Modification of Network Configuration

- Network resources are generally not modifiable if being used by other resources. This provides the necessary level of protection needed. However, there are potentially situations where this is not the case and additional separation controls may be introduced at a later date.