Policy Monitoring and Enforcement Strategies

Erika Hernandez

NET 3730 Cyber Policy and Ethics

Professor Paulson

November 28, 2021

Policy Monitoring and Enforcement Strategies

In this paper we will be describing the policy monitoring and enforcement strategy in the organization. We will be identifying and will be describing the legal implications of ISS policy enforcement after the modified policies are adapted. Along with breaking down the scenario working for the Department of Defense (DoD).

Level 1 Heading

Imagine working for the Department of Defense (DoD). Sitting here thinking what would that look like? Working for the DoD is a level of security, they are over the Army, Navy, The Air Force, and The Marine Corps. So this means that they have to have lots and lots of security. They are handling lots of important and highly classified information. Having said that, the bottom line is they have to be secured. With the products weapons and other highly classified equipment, in the wrong hands can cause some high and devastating issues.

With this highly secure information and secure information passing through the DoD. They would need a remote access policy in place. With all federal employees working around the world and working within the organization. They need to have guidelines on remote access and policies. They need to have secure passwords, with the guidelines along with it. Certain people would have certain clearance and certain people are given certain access.

Along with the remote access policy, they would have to know that when traveling and or around certain places that they will be monitored. They would have to use multiple levels of authentication. Those that are securing certain things would have some people securing them. The devices that are being used would also have to have and or be given permission by the DoD secure team.

Buying equipment and or building certain weapons would also have to have a certain level of security. Having the remote access policy would let everyone know the policy on who can make those types of orders or buy those types of things. To have a non-supervisory union would make sense as well. Most of these staff are and have gone through extensive backgrounds to ensure they can be trusted. So it would make sense that they are not being super micromanaged, but they have tons and tons of policies that they have to follow. That is where I feel is the kicker of freedom. If they go outside of those various policies it will cost them issues.

The magnitude of employees whether it be 50 or 7000 employees would not make much difference when it comes to this level of security. Not to say that is not a concern it comes down to going into very specific detail on what is expected of all those employed by the DoD. With the remote access policy, some Information security policies would also be implemented to make sure that only specific things can be talked to. Knowing who and what clearance people have to know the information.

Contractors would have a different type of remote, information, and security policy. Their wording would be different because of their contracting status they would only have to have specifics on what is needed. They would not and should not have another type of information given per the policies. In some of the documentaries that Nasa has to contract out, they don't even know what government is requesting the product or order. All they know is the government wants this equipment.

Also having around 35 locations throughout the United States is something else to factor. Secure VPN and the DoD would also have other security policies for software applications. These will have a controlled element to them as well. Very strict access will only be allowed to certain people. The higher clearance a person has the more sensitive the information they will have. The lower security clearance the less information they will have. This is due to the militarily and important information that the DoD carries.

Conclusion

Overall, this scenario is a pretty good way to think if you are put into an startup organization, to see what kinds of securities are being implemented in the organization. This is a very realistic scenario to know going into a company, But not for or an organization for like DoD, the DoD was progressed as the technology did as well. New Cyber threats are constantly evolving and an especially for an organization like the DoD. They would have to always be one step a head of new threats that can be departmental for the country and its safety.

Having said that, security personal that are over the network infrastructure need to have polices in place. They also need to have the people that need to know and what type of sensitive information they are carrying. But also not over look even those contractors as well. All employees need to know the rules and polices that are being placed for the organization. Also, they need to be revised as technology progresses, and is evolving.

References

DoD Org chart: U.S. Department of Defense insights. (n.d.). Retrieved from https://www.orgcharting.com/dod-org-chart/