Cameron Waddy

UIN: 01155896

Professor Fateh

December 8, 2020

ODU Computer Policy

Old Dominion University (ODU) has their online computer security policies written and maintained by the Information Technology Advisory Committee (ITAC). This committee is appointed by the university and represents constituents throughout the campus. They have a multitude of responsibilities that result in the maintenance of this special policy. Even though ITAC is the specific committee for this set of policies, it must be approved by many other committees and counsels. This is to ensure a strong and secure set of policies that are effective.

ITAC meets on the first and third Tuesday of every month at 8:30 AM in Gornto Hall. The first of this counsel's responsibilities is that they, "Provide advice and recommendations to the University's administration concerning technology strategic directions, operating policies, and student, faculty and staff technology needs." (ODU, 2020) The next responsibility of the ITAC is to keep the Old Dominion community informed about any technology issues or new initiatives being introduced. This could involve Blackboard, our University's class navigation and online school application, going down or crashing. The third of its many responsibilities are to advise IT on the policies, procedures, and the University standards for keeping all of its sites and applications running fluently, safely, and securely. Also, the committee will make recommendations on other IT related decisions within the perspective of the University and provide further leadership and guidance towards the new implementations of IT policies and procedures. This special committee can be considered the big picture committee when it comes

to computer safety and policy. Not only do they work on projects themselves, but they provide oversight, involvement, and direction while also working as sponsors for newfound IT initiatives. Nothing would be completed without the help and oversight of the Information Technology Advisory committee. I believe that it would be a big understatement to just say that this committee is important. They involve many different people comprised from all of the different offices and colleges within Old Dominion University.

Information technology policies, procedures, and guidelines are put together to guide and direct the University's practices. They are also put together to ensure compliances with any and all laws, regulations, and requirements to reach long-term goals. But how do we know when a change has occurred, or a change is needed to be completed in accordance with these laws, regulations, or requirements? We can know, based off of a change in the law, rule or regulation or if there is a weakness or deficiency in the current structure. Some other ways we will receive a change, are if there is need to correct or reduce behavior, if there is an organizational change, in order to streamline operations, as well as any new technical opportunities or recurring periodic reviews and updates. All of these different potential changes will be reviewed and taken care of by none other than ITAC.

There are nine total policies that pertain towards technology use in general computer, back-end software and management, as well as security. The purpose of policy 3500 pertains to computing resources. These resources are meant to give information for the computer users about the responsibilities in using the information technology at ODU. The next policy is 3501 which tells us who will be able to access these IT resources. This guidance restricts and controls the availability of certain and all information and whether it is available to the general public, students, or the administrators. This will vary and could include a mass amount of people down

to a select few with extremely restricted access. For policy 3502, it is more of a promise or commitment to hold oneself responsible for establishing and the already established guidelines, standards, and procedures that affect key components pertaining to IT infrastructure, architecture, and all of its ongoing operations. (ODU, 2018) Policy 3504 is to "establish framework for administering the University's institutional data." (ODU, 2018) The *Information Technology Security Policy* is policy number 3505. "The purpose of this policy is to state the codes of practice with which the University aligns its information technology security program and document the best practices and standards with which the University aligns its security activities." (ODU, 2018) This is just a glimpse into the policies to give you an idea about what the University has put into place to ensure a safe environment and experience for all IT users. For your information, the last four policies listed are *Electronic Communication Policy for Official University Business* (Policy 3506), *Information Technology Accessibility Policy* (Policy 3507), *Information Technology Project Management* (Policy 3508), and the final policy is *Software Decision Analysis Policy* (Policy 3509). It should be noted that Policy 3503 is not a policy that is being referenced for computer security at this time.

There is not only one group watching over all of these policies. There are more groups/people similar to the Information Technology Advisory Committee. There are a multitude of councils and committees that have to approve the work that ITAC has done. These councils and committees are the Policy Formulation Committee, the Policy Review Committee, the Executive Policy Review Committee, the University Counsel, and then finally the University president. All of the policies that have been passed, not just the computing policies, must be reviewed and approved by each in order to be mandated. However, not all procedures are published for the public record. The reason is not to hide in secrecy but to provide for better

security for all users. Even though these procedures and guidelines are not published, it is still possible to obtain them. Obtaining these guidelines can be done by submitting a request to the operational unit, whereupon the submission can be received, and the requested documents can be provided.

The process of completing a review and approval for the online computer security policies is a sophisticated but efficient one. Each policy is thought through carefully by examining all of the details to ensure a strong, safe, and understandable policy that can be maintained and enforced effectively. Overall, these policies provide a secure, dependable, and efficient use of all ODU computers, users, and their systems software. ITAC does a professional job enforcing and writing these policies along with the associating committees that legitimize the proposed policies.

Bibliography

"3500: Policy on the Use of Computing Resources." *Old Dominion University*, www.odu.edu/about/policiesandprocedures/university/3000/3500.

"3501: Information Technology Access Control." *Old Dominion University*, www.odu.edu/about/policiesandprocedures/university/3000/3501.

"3502: Information Technology Infrastructure, Architecture and Ongoing Operations." *Old Dominion University*, www.odu.edu/about/policiesandprocedures/university/3000/3502.

"3504: Data Administration Policy." *Old Dominion University*, www.odu.edu/about/policiesandprocedures/university/3000/3504.

"3505: Information Technology Security." *Old Dominion University*, www.odu.edu/about/policiesandprocedures/university/3000/3505.

"Computing Policies." *Old Dominion University*, www.odu.edu/about/policiesandprocedures/computing.

"Information Technology Advisory Council (ITAC)." *Old Dominion University*, www.odu.edu/its/advisory-committee/itac.