NAME: Rick Lambert

ORGANIZATION: University of South Carolina

PROJECT TITLE: VPN Access Process

DATE: 1/24/20

**Problem Statement:**

The goal of this project is to examine the request process for Virtual Private Network (VPN) access to sensitive systems on campus. A VPN allows access to systems on campus that may contain sensitive information or to systems on campus from remote locations in a secure manner. Unauthorized access could pose a threat to the system in question or the information contained/processed by that system.

This project aligns with the University of South Carolina's Division of Information Technology Strategic Priorities as stated below:

**Strategic Priority 1**

Advance the academic and research missions of the university

*The preeminent priority of the Division of Information Technology will be to make substantive contributions to the teaching and research missions of the university.*

**Strategic Priority 3**

Improve administrative efficiencies

*We will work to streamline administrative systems and processes to minimize overhead and duplicated work.*

**Strategic Priority 5**

Provide a reliable and flexible technology infrastructure

*The Division of Information Technology will plan for future growth and innovation by providing a technology infrastructure that can be expanded, upgraded, and replaced to meet growing needs.*

(https://www.sc.edu/about/offices_and_divisions/division_of_information_technology/about_us/strategicpriorities/)

Currently users request access to a specific VPN and access is granted based on an informal approval process, typically through an email or phone call to someone in Network Services. There is no documented process to verify the validity of the request or to make a record of the approval process.

**Data Collection:**

The goals of the data collection were to establish the number of known VPN groups, the members of each group and any information known about the group owners. Another goal was to establish the current process for requesting and granting access to a VPN group. All information on VPN groups, owners and users, as well as, approval processes were gathered from the Network Services group which maintains the VPN for the University of South Carolina.

| Term | Definition |
|---|---|
| VPN | Virtual Private Network allows access to systems on campus that may contain sensitive information. Each system has its own VPN group to control access by users. |
| VPN Group | Group of users who have access to a VPN |
| VPN Group Owner | Person responsible for the users who have access to a VPN. They have the authority to make changes to access, approve user access and request users be removed from the group |
| VPN User | Has access to systems that require VPN access. They must request access to specific systems before they are added to the VPN group. |

**Data Analysis:**

Analysis of the data revealed that the information maintained on the VPN groups was incomplete or inaccurate in some cases. There was no formal process to maintain the contact information on the groups or the users. There was no information kept on who requested the groups to be created. Information on the identity of the group owners was incomplete and there was no periodic verification that all the users in the groups still needed access to the data.

Potential causes of the data inaccuracies can be linked to no formal process being in place to create or modify VPN group membership. Also, there is no central database maintained to house the data that is collected. Lastly, there is no formalized database to house the information from the original VPN requests as they are received and completed.

This project would establish a VPN group owner for each VPN group who will have authority to grant or remove user access to the group. This project would also verify the users who will be members in each VPN group. The information on VPN groups would be housed in a centralized content management database. Next, formal processes would be established for the maintenance of the VPN groups. Users would complete a formal request for access through a service management software. The request would be approved or denied by the VPN group owner. Based on the approval status within the process, users would be granted access to the VPN group.

**Implementation Plan:**

1. Verify the list of VPN groups with their owner or known contact.
    a. Assemble the list of active VPN groups from the VPN management software- Network Services (8 hours)
    b. Establish a list of possible VPN group owners by consulting with the network technicians or by relying on institutional knowledge based on past experience- Network Services (8 hours)

c. Contact each potential VPN group owner to verify that they are still associated with their VPN group and that they are authorized to approve or deny users access to their group. If they are not the appropriate person, inquire as to who might be the correct contact. Network Services/VPN users (24 hours)
d. Document the findings in a VPN groups database to be maintained for VPN access- Network Services (4 hours) (*See VPN Group Informational Database, p12)*
e. Potential obstacle- The list of VPN groups is maintained within the VPN management software, however there is no formal group of VPN owners. Given the methods employed in the past to establish groups and members, information may be lost or unavailable at this time. Some group owners may be identified from memory while others may have to be established by a process of elimination.
f. Potential method to overcome- Each potential group owner will be contacted to verify they are still working with the group and to establish themselves as the contact with the authority to police the users within the group.

2. Verify the list of VPN users for each group
    a. Assemble a current list of VPN users for each group- Network Services (8 hours)

b. Verify that each current user listed in the VPN group is approved by the group owner. Remove any users who are no longer approved for access- Network Services/VPN users (40 hours)
c. Document the findings in a VPN groups database to be maintained for VPN access- Network Services (4 hours) *(See VPN Group Informational Database, p12)*
d. Potential obstacle- The list of VPN groups is maintained within the VPN management software, however there is no formal process to remove users who may no longer need access. Users may still be employed by the university or within the same group, but their need for access to sensitive information may have changed since their original access to the group was granted.
e. Potential method to overcome- Each potential group owner will be contacted to verify the list of known users for the group they are responsible for. The VPN group owner will need to verify that each user is authorized to continue access to the group.

3. Establish an approved process to add or delete users for VPN groups
    a. Verify the steps to adding or deleting users from VPN groups- Network Services (8 hours)
    b. Verify requirements for the necessary information needed to complete a request for access to a VPN group- Network Services (8 hours)

c. Establish the VPN request process as a workflow in the service management software to create a ticket for each request- Network Services (40 hours) (*See VPN Add User Workflow, p13, VPN Delete User Workflow, p14)*

d. Create a formal request with the service management team to convert the VPN request process into a workflow that can be maintained in the service management software. This would allow potential VPN users to complete a ticket, with the required information, where the request would be managed through the service management software. Network Service/Service Management (80 hours)

e. Potential obstacle- Users who are accustomed to making requests via phone or email may be unwilling to submit requests through a service management software service. It will take time to establish the process of requiring all information up front and in a ticket form to process a request.

f. Potential method to overcome- Communicate with the VPN groups, as well as, other groups on campus who may be affected by this change in procedure. Identify the positive outcomes of the new process and how it will make the protected systems more secure in the future. Also, allow Network Services to create tickets on behalf of the customers in the beginning to help them become accustomed to the new process.

4. Establish a centralized location for the VPN group information to be housed.
    a. Create a formal request with the service management team to store the VPN groups database in the content management database- Network Services (4 hours)
    b. Establish guidelines on access to the information in the database based on security parameters set forth by university policy- Network Services/Service Management/University Information Security Office (20 hours)
    c. Establish a process, either manual or automatic, to update the information in the database based on requests to add or delete users- Network Services/Service Management (40 hours)
    d. Establish a periodic review plan with the VPN group owners to verify that all users accessing the VPN are authorized to do so- Network Services/VPN Users (8 hours)
    e. Potential obstacle- The initial list of group owners and users will be up to date when created. The potential to maintain edits to the list automatically based on the requests received through the service management software is unclear.
    f. Potential method to overcome- Consult with service management team on the capabilities of maintaining changes automatically through the request process. Identify any gaps and address issues

with the service management software vendor to be resolved in upcoming software releases.

5. Establish a communication plan to notify users who may be affected by the changes in procedure.
    a. Establish an informational document detailing what users should expect when the new process goes into operations. Knowledge based articles and other FAQs may provide valuable information and reduce confusion. Provide a method for users to contact Network Services for questions that may not be covered in the documentation provided- Network Services/Service Management (40 hours)
    b. Using the contact information gathered while verifying the current group owners and users, create a communication list to inform users of the upcoming changes to the process and where users can get more information on what to expect- Network Services (16 hours)
    c. Working with Communications, establish the methods to communicate with the users, the frequency of the communication and the places where information will be available- Network Services/Communications (24 hours)
    d. Potential obstacle- reaching all users via email or other written method requires the user to take the time to read the communication. Accessing the VPN may be a very small portion of

the user's actual job and therefore, they may choose to ignore emails or posted messages.

e. Potential method to overcome- Communicate the changes to the group owners, group members, network managers and any other group that may have VPN access. Work with the VPN group owner to assure that they have made their group members aware of the upcoming changes. Make the information available via Knowledge Articles that can be searched through the service management software.

6. There is no outside cost associated with this proposed change. The VPN management software that contains the information is already in use. The service management software is in use and the functionality already exists. Time estimates and resources are noted at the end of each task.
7. Integration into standard operating procedure only requires the request for approval of the process and the development of the processes into a service management workflow.

**Evaluation Method:**

Periodic review of the content management database should be conducted at least annually to verify that the group owners and users are still authorized to access the data from the VPN. This review should also verify contact information and assure that the VPN is still in use.

The review would require Network Services to reach out to each VPN group owner and conduct the review either in person or through email. Verification information should be stored within the content management database.

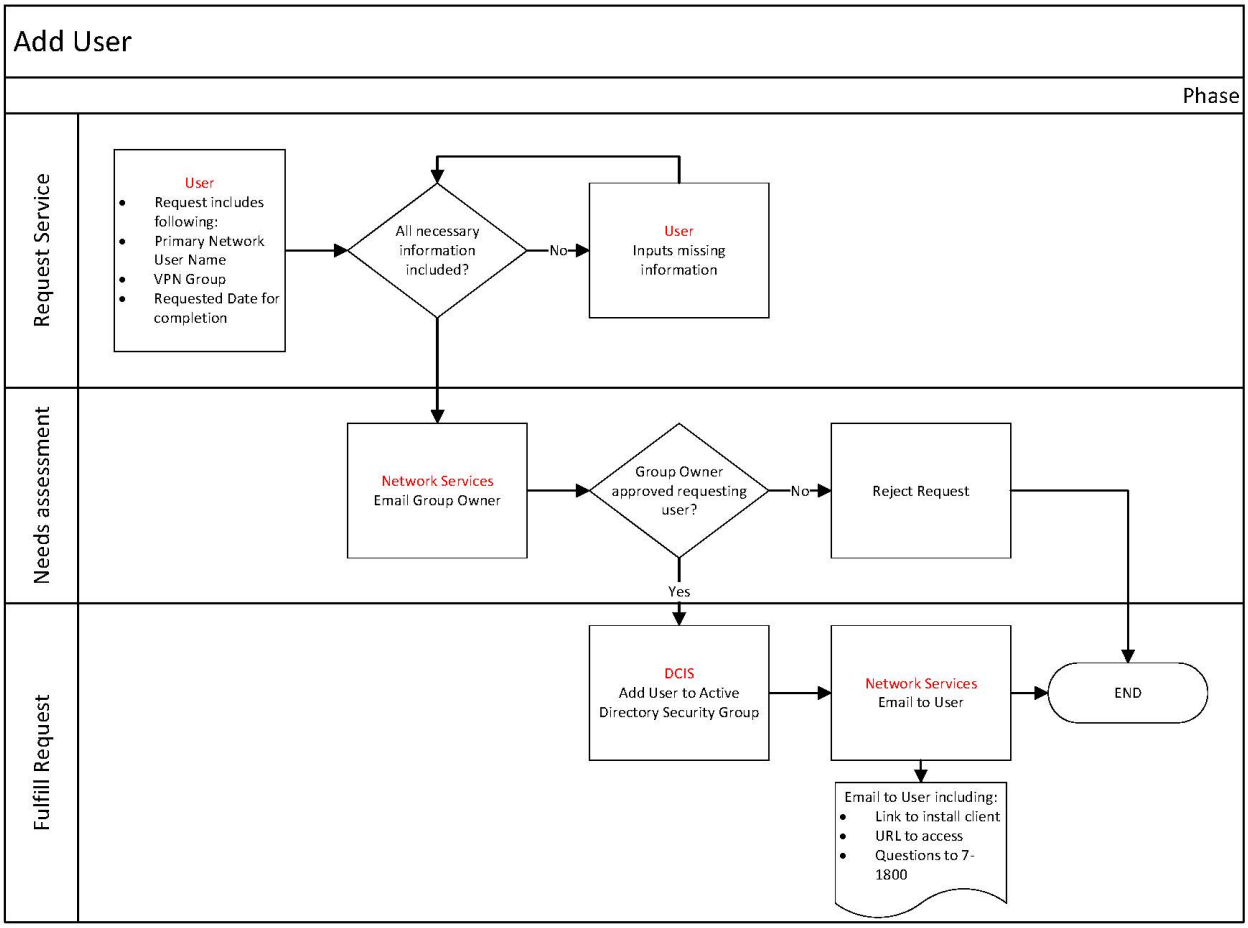
**Summary and Recommendations:**

User access to sensitive data is an important topic to consider in todays cyber security driven workplace. In this case, the information was sporadically available, but not stored in a centralized location. The information was not reviewed with any regularity and access to data was largely at the discretion of the technician instead of the group owner. The management of users within a VPN group is only the beginning. Other processes could be integrated with this method beginning with the creation of VPN groups or the deletion of VPN groups that are no longer needed. The entire process of maintaining VPN groups should be migrated into the service management software to allow technicians to store information on requests dealing with VPN groups. This type of process would also be beneficial to other types of requests made to the Division of IT to ensure that there is a clear sequence of requests detailing any changes that are requested for future reference.

## VPN Group Informational Database

| Group Name | Member Count | Group Owner | Member Names |
|---|---|---|---|
| VPN-1 | 10 | VPN Owner 1 | User 1 User 2 User 3 User 4 User 5 User 6 User 7 User 8 User 9 User 10 |
| VPN-2 | 2 | VPN Owner 2 | User 11 User 12 |
| VPN-3 | 7 | VPN Owner 3 | User 13 User 14 User 15 User 16 User 17 User 18 User 19 |
| VPN-4 | 6 | VPN Owner 4 | User 20 User 21 User 22 User 23 User 24 User 25 |
| VPN-5 | 6 | VPN Owner 5 | User 26 User 27 User 28 User 29 User 30 User 31 |
| VPN-6 | 6 | VPN Owner 6 | User 32 User 33 User 34 User 35 User 36 User 37 |
| VPN-7 | 22 | VPN Owner 7 | User 38 User 39 User 40 User 41 User 42 User 43 User 44 User 45 User 46 User 47 User 48 User |
| VPN-8 | 10 | VPN Owner 8 | User 60 User 61 User 62 User 63 User 64 User 65 User 66 User 67 User 68 User 69 |
| VPN-9 | 16 | VPN Owner 9 | User 70 User 71 User 72 User 73 User 74 User 75 User 76 User 77 User 78 User 79 User 80 User |
| VPN-10 | 81 | VPN Owner 10 | User 87 User 88 User 89 User 90 User 91 User 92 User 93 User 94 User 95 User 96 User 97 User 98 User 99 User 100 User 101 User 102 User 103 User 104 User 105 User 106 User 107 User 108 User 109 User 110 User 111 User 112 User 113 User 114 User 115 User 116 User 117 User 118 User 119 User 120 User 121 User 122 User 123 User 124 User 125 User 126 User 127 User 128 |
| VPN-11 | 57 | VPN Owner 11 | User 169 User 170 User 171 User 172 User 173 User 174 User 175 User 176 User 177 User 178 User 179 User 180 User 181 User 182 User 183 User 184 User 185 User 186 User 187 User 188 User 189 User 190 User 191 User 192 User 193 User 194 User 195 User 196 User 197 User 198 |
| VPN-12 | 0 | VPN Owner 12 | |
| VPN-13 | 1 | VPN Owner 13 | User 226 |
| VPN-14 | 2 | VPN Owner 14 | User 227 User 228 |
| VPN-15 | 97 | VPN Owner 15 | User 229 User 230 User 231 User 232 User 233 User 234 User 235 User 236 User 237 User 238 User 239 User 240 User 241 User 242 User 243 User 244 User 245 User 246 User 247 User 248 User 249 User 250 User 251 User 252 User 253 User 254 User 255 User 256 User 257 User 258 User 259 User 260 User 261 User 262 User 263 User 264 User 265 User 266 User 267 User 268 User 269 User 270 User 271 User 272 User 273 User 274 User 275 User 276 User 277 User 278 |
| VPN-16 | 5 | VPN Owner 16 | User 326 User 327 User 328 User 329 User 330 |
| VPN-17 | 17 | VPN Owner 17 | User 331 User 332 User 333 User 334 User 335 User 336 User 337 User 338 User 339 User 340 |
| VPN-18 | 11 | VPN Owner 18 | User 348 User 349 User 350 User 351 User 352 User 353 User 354 User 355 User 356 User 357 |
| VPN-19 | 3 | VPN Owner 19 | User 359 User 360 User 361 |
| VPN-20 | 2 | VPN Owner 20 | User 1 User 2 |
| VPN-21 | 7 | VPN Owner 21 | User 3 User 4 User 5 User 6 User 7 User 8 User 9 |
| VPN-22 | 5 | VPN Owner 22 | User 10 User 11 User 12 User 13 User 14 |
| VPN-23 | 16 | VPN Owner 23 | User 16 User 17 User 18 User 19 User 20 User 21 User 22 User 23 User 24 User 25 User 26 User 27 |
| VPN-24 | 12 | VPN Owner 24 | User 32 User 33 User 34 User 35 User 36 User 37 User 38 User 39 User 40 User 41 User 42 User |
| VPN-25 | 30 | VPN Owner 25 | User 45 User 46 User 47 User 48 User 49 User 50 User 51 User 52 User 53 User 54 User 55 User 56 User 57 User 58 User 59 User 60 User 61 User 62 User 63 User 64 User 65 User 66 User 67 |
| VPN-26 | 1 | VPN Owner 26 | User 76 |
| VPN-27 | 0 | VPN Owner 27 | |

## VPN Add User Workflow



## VPN Delete User Workflow