Dunbar Alumni Federation, Inc. • P.O. Box 60714 • Washington, DC 20039

NEED -TO - KNOW POLICY

DEFINITION

'Need to know' principle is self-explanatory, and as per the Urban Dictionary means 'information is only given to those who can present a good case for knowing about it. It describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary approvals to access certain information, one would not be given access to such information, unless one has a specific need to know, that is, access to the information must be necessary for one to conduct one's official duties. This term also includes anyone that the people with the knowledge deemed necessary to share it with.

ACCESS CONTROL

The Chair and the Designated Manager(s) have total access control and can pass access permissions to individuals on all systems and/or programs utilized by the organization. The list includes but is not limited to customer relationship management, financial management oversight, communication venues, technology partners as well as organizational fundraising entities. These permissions are granted based on the need to know in the performance of the individual roles and responsibility. User access classifications may include total or managerial access (Administrator), partial access (User/Editor) or very limited (Limited User). The need-to-know is a data security mechanism.

USER CLASSIFICATION

A user is defined as any volunteer or employee of the organization. They shall only have access to the information that their function requires. Further, a user needs permissions AND a need-to-know. The need-to-know access is strictly bound to a real requirement for the User to fulfill their current role. When a user changes role, DAF will adjust the need-to-know access immediately.

USER ACCESS

DAF implements its Need-To-Know Policy by granting minimum access rights to information. Therefore, when higher access rights are necessary, volunteers/employees are granted these rights based on their needs. By granting access rights this way, usage of these privileges including the activities performed on the data can be closely monitored, and once the requirement ceases, these rights can be revoked, if applicable.

METHODS

'Need to know' vs. Authorization

The 'need-to-know' and 'authorization' are very closely associated and in some cases, they are even used interchangeably. In general, a demonstration of the 'need to know' is required to get

authorized. Yet, even when an authorization approval is acquired, it will not necessarily mean that one is qualified with a 'need to know' for the information they seek.

Need to know' as a function of time
'Need to know' can be described as a function of time. The 'needs' may varying from one situation to another making it very costly to control at runtime.

'Need to know' implemented through 'trust'.
An organization with highly sensitive data enforces the 'need to know' objective through a mechanism of 'trust' placed upon a volunteer/employee. First, a control to establish the 'trust' is enforced and once that control is passed, the trust in the volunteer/employee's integrity is used to manage the 'need to know' objective.

'Need to know' implemented through granting minimum rights to information.
Another organizational model of implementing the 'need to know' principle is by granting minimum access rights to information. Therefore, when higher access rights are necessary, volunteers/employees are granted these rights based on their needs. By granting access rights this way, usage of these privileges including the activities performed on the data can be closely monitored, and once the requirement ceases, these rights can be revoked

CONCLUSION
As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. Need-to-know also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people. Failure to adhere to the Need-to-Know Policy may result in removal.

I, _____, have read and understand the above expectations of the Dunbar Alumni Federation, Inc. and agree to abide by this Need-To-Know Policy.

_____ _____
Signature Date