Procedure Title: **Establishing an ACF2 Account**
Document Number: **110201-P-035**
Revision: **1.0**
Process Owner: **DTI Chief Security Officer**
Date: **April 30, 2009**

Table of Contents

Date Changed	Revisions	Changed By	Revision #
Original	Base lined		1.0

1.0 Scope

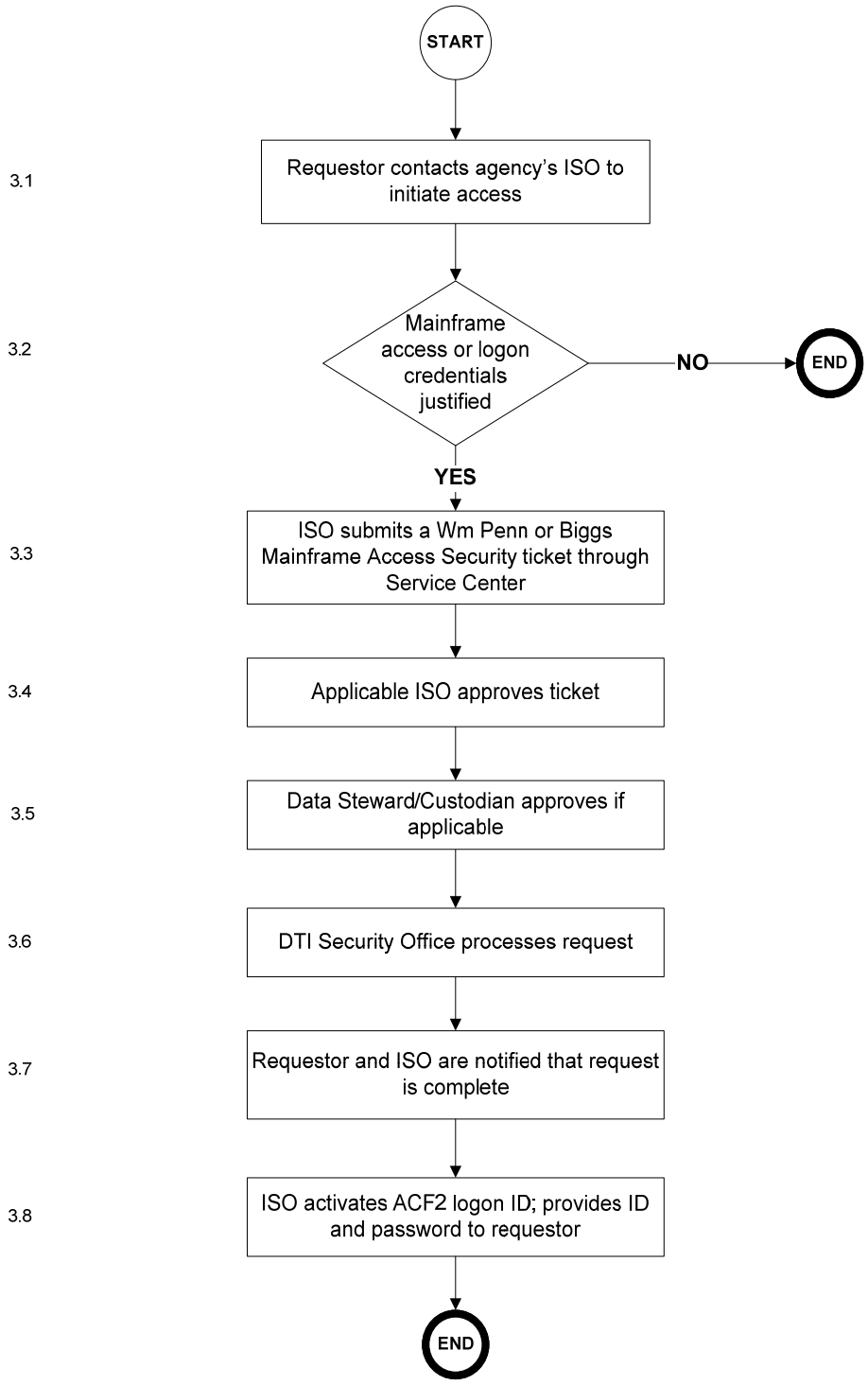
This procedure defines the process for requesting an ACF2 account and logon credentials. An ACF2 account must be established to gain access to mainframe applications. This process applies to State organizations (State agencies, K12, Higher Education, etc.).

Note: K12, Higher Education and other organizations that do not have access to the State domain must also acquire a Secure Socket Layer-Virtual Protocol Network (SSL-VPN) account to gain access to state resources from outside the network.

An ACF2 account is requested through a requestor's Information Security Officer. Each organization's or school district's Information Security Officer (ISO) has been trained to request access and logon credentials. Requests are submitted through the Service Center application and processed by the DTI Security Office.

This process is triggered when it is determined that access to a mainframe application is required as a part of the requestors job related duties.

2.0 Process Flow Diagram



3.0 Procedure

3.1 Requestor contacts their Information Security Officer (ISO) and requests that they initiate the process to establish an ACF2 account.

3.1.1 Requestor could be an employee or an employee's supervisor. If you are not sure who the ISO is for your organization, refer to DTI's Extranet, How Do I section – Find my ISO.

3.2 Requestor's ISO verifies that the requestor requires access to mainframe applications in order to perform their job related duties or logon credentials are required for other applications. If so, proceed to 3.3

3.2.1 If access is not warranted, end of process.

3.3 Requestor's ISO accesses DTI's Service Center and completes a security ticket (Security Forms/William Penn or Biggs Mainframe Access) to obtain ACF2 logon ID and password for requestor.

3.3.1 ISO selects forward and the ticket is moved to the ISO Approval phase.

3.4 Applicable ISO approves ticket.

3.4.1 Ticket is forwarded to the Data Steward Approval Phase if applicable.

3.4.2 If not applicable, ticket is forwarded to DTI Security Office's queue, Step 3.6

3.5 Data Steward/Custodian approves the ticket.

3.5.1 Ticket is forwarded to DTI Security Office's queue.

3.6 DTI Security Office processes the ticket according to ISO's specifications and closes it.

3.7 Requestor and his/her ISO receive a Service Center email indicating that the request/ticket has been completed.

3.8 The ISO activates the ACF2 logon ID and provides the requestor with the password.

3.8.1 How the individual requestor is informed of their password is dependent upon requesting organizations internal operating procedures, but it must be in compliance with the Delaware Information Security Policy (DISP).

3.9 End of process

NOTE: K12, Higher Education and other organizations that do not have access to the State domain must also acquire a Secure Socket Layer-Virtual Protocol Network (SSL-VPN) account to gain access to state resources from outside the network.

Please refer to the process for acquiring access to the State's telecommunication network using Secure Socket Layer – Virtual Private Network (SSL-VPN).

4.0 Reference Documents

110305-P-002 Access the State of Delaware telecommunications network using Secure Socket Layer – Virtual Private Network (SSL-VPN) State and K12

Delaware Information Security Policy

Information Security Officer (ISO) List