





Operation/Task:	FireID Network Account for Use by Developers			Equipment:	Production Servers
Owner:	Vice President of Technology	Date Prepared:	02/12/20	Department:	Information Technology
		Revision History:	See last page		

ALERTS (see below): Critical Step  Quality Check  Tip  Team Safety 

Purpose: Access to servers containing client data for developers is prohibited by Developers while they are using their standard login accounts. Administrator-level accounts have been created for each Developer for their occasional required access to these servers. These local administrator account names are denoted by the Developer's initials plus the prefix of "FireID." These FireID accounts are placed into specific groups in AD which are named "LA_" plus the server name. Developers use their normal user accounts for day-to-day work and will only use their FireID Accounts when absolutely required to complete the project at hand.

Step #	Alerts	Step Description - "What to Do"	"How to Do it"	"Why to Do it"
1		Record FireID access in TrackIt	Each month the Vice President of Technology creates a new TrackIt ticket to log all of the month's FireID usage. Attached to this ticket is a log spreadsheet to track each FireID use.	This explains the reason for the FireID use and enables their manager to monitor this access.
2		Logging in to a production server	Developer logs in using their FireID account which is configured to utilize MFA for windows RDP.	This separates regular daily development and maintenance tasks from production troubleshooting.
3		Alert to usage of the FireID	The Security Information and Event Management (SIEM) system sends an email alert to all CAPS team members whenever a FireID is used to access a server that contains non-anonymized client data.	This notifies the relevant compliance staff that a FireID is logged into a server.
4		Compare FireID usage	The TrackIt tickets and alert emails are correlated, with any missing information updated in TrackIt.	This validates that all FireID usage is being properly documented in TrackIt.

5		Review FireID TrackIt	The manager of the Developers and/or any CAPS committee member reviews new FireID usage and updates the monthly TrackIt ticket with the FireID usage event.	This validates the reason for the FireID use.
6		Ownership by Developer's Manager	The Developer's manager closes the ticket after the month's end.	This allows the Developer's manager to validate the ticket and keeps our ticketing system clean.
7		Monthly CAPS discussion	Vice President of Technology leads a discussion on FireID usage at least monthly at CAPS meetings.	These discussions keep this top-of-mind for all CAPS members to continually act as a compensating control regarding developer access.

Notes:

Definitions:

Revision History	Description of Changes	Requested by	Date
Rev 1	Initial version	Dave Johnson	02/12/20
Rev 2	Wordsmithing, minor editing and adding CAPS oversight.	Frank Powell	02/13/20
Rev 3	Addition of ticket ownership responsibilities for Developers' manager.	Frank Powell	2/17/20
Rev 4	Changed gray header owner and date information	Cristi Oakvik	4/14/20
Rev 5	Changed GLS reference to ENPOINTE	Cristi Oakvik	3/9/21
Rev 6	-Modified step #1 to include MFA required with FireID login -Changed SIEM from AlientVault to Blumira -Modified Step 2 - Developer selects "FireID" from the dropdown in the "Subtype field"	Danette Colin	10/10/22
Rev 7	Changed owner to Director of Business and Custom Applications Updated steps to reflect updated process of using a monthly TrackIt ticket instead of daily.	Mike Starrett	5/5/23

Rev 8	Updated owner to Vice President of Technology	Mike Starrett	11/4/24
-------	---	---------------	---------