Users with Personal PIN

	New	Active with contact info	Active, no contact info	Inactive >495 days
CONVERSION DATE				LOCKOUT
	n/a	no change	no change	account locked, must follow reset PIN instructions based on system contact info status

(normal course of business)

PIN resets

	Active with contact info	Active, no contact info
CONVERSION DATE		
	Temporary (1x) PASSCODE provided via call, email or text to unlock account and reset PIN within the app	Redirect to CSR for eID authentication, a pass = CSR unlocks account and sets back to default PIN for user login and change to personal PIN
	Temporary PASSCODE expires w/in hours, Default PIN restoration expires in 3 calendar days	

with Default PIN

	New	Active with contact info	Active, no contact info	Inactive >495 days
CONVERSION DATE		LOCKOUT	LOCKOUT	LOCKOUT
	within 30 days of user upload, entry of a default PIN to set up an account access	forced user change to personal PIN upon next login via PASSCODE reset in app	forced user change to personal PIN upon next login, redirect to CSR for eID authentication and set back to default PIN	account locked, must follow reset PIN instructions based on contact info status
	Temporary PASSCODE expires within hours, Default PIN restoration expires in 3 calendar days			

LOCKOUT RECOVERY PROCESS (USER):

follow PIN reset instructions on the login screen

a temporary passcode (1x only use, expires within hours) is sent via the user-selected method

if reset contact info is not available, login screen will redirect to CSR

CSR will use eID questions to authenticate user, unlock the account and restore default PIN (1x use, expires in 3 days)

if user fails the eID questions, the CSR will redirect user to employer contact to authenticate

NOTE: The employer web manager can authenticate, unlock the account and reset to the default PIN