Comments on Minimum Security Standards from TAC Dist List Members

ID items for discussion in TAC PowerPoint

Date Rec'd	Received from	Comment Content	AOC Response
1/26/16	Jay Dennis	Local systems have no way to enforce 2 alpha and/or 2 numeric passwords	Should be changed to "where possible".
1/26/16	Jay Dennis	There needs to be provisions to allow for on-call staff. Pro tem judges may not appear in court within 30-day time frame and therefore be revoked.	Make exceptions of the one off's somehow or extend the account deletion time to a longer period
1/26/16	Jay Dennis	Local leadership unable to reduce 90 day password change to 60 day requirement	DPS requirement is 60 days, but could be changed to 90 days for those not feeding DPS
1/26/16	Jay Dennis	Court unable to meet every 6 month password change requirement for service accounts	Should be changed to 1 year. It's not done today typically.
1/26/16	Randy Kennedy	Scottsdale has password changes set at 90 days	See above
1/26/16	Randy Kennedy	Scottsdale locking screen savers set at 30 minutes after judges complained of having to constantly login while on the bench with 5 minute setting	User can override default time but not allowable to not have locking screensaver
1/26/16	JGilbertson	Required fire suppression signage (FM-200) on door is a dead giveaway, though data center not formally labeled. Is that an issue?	Law requires denote fm-200 or any fire suppression system in place
1/26/16	JGilbertson	Phoenix user access handled by HR process during hiring may not exactly follow the required written request and approval process	There is no need for a full incident management system as long as requests are documented and a process is being followed and validated
1/26/16	JGilbertson	Phoenix inactive userIDs reviewed for deletion at 90 days rather than required 60 days	Change this to 90 days

Date Rec'd	Received from	Comment Content	AOC Response
1/26/16	JGilbertson	Phoenix transfers terminated users' files to supervisor but doesn't automatically purge them 4 weeks after termination	4 weeks is a best practice to keep old files from accumulating – there needs to be an upper limit
2/1	JNishimoto	Password should include 1 special character	Unfortunately, some of the older systems (AS/400) won't take special characters
2/1	JNishimoto	IDs should be reviewed for deletion after 90 days, not 60.	See above
2/1	JNishimoto	"files from non-Judicial-Branch sources are screened with virus detection software" – what software product?	Mainstream ones in the EA table, most notably McAfee
2/1	JNishimoto	Where are the "defined vulnerabilities that are to be remediated immediately" made available?	This is tricky and varies by risk/impact. "High & Critical" vulnerabilities should be remediated immediately
2/16/16	Kyle	User Access & Controls section does not specifically identify if the items are for domain authentication or all systems – cant' go further without knowing scope	It includes AOC systems as well as local systems. AOC is evaluating itself against the criteria rather than setting them by its present capabilities.
	Kyle	Formalize how to notify or receive AOC approval – can't be just sending e-mail to Rod Franklin	Needs to be a Remedy request