



one COUNTY | one FUTURE

Legislation Text

File #: 21-00847, **Version:** 1

Consider recommendations regarding Countywide Technical Cyber Security Policies, as follows:

a) Approve the following 20 Technical Security Policies:

- i) IT Security Program Description (ITAM-0600);
- ii) IT Security Program Implementation Plan (ITAM-0601);
- iii) Glossary of IT Security Terms (ITAM-0602);
- iv) Access Control (AC) (ITAM-0610);
- v) Awareness and Training (AT) (ITAM-0611);
- vi) Audit and Accountability (AU) (ITAM-0612);
- vii) Security Assessment and Authorization (CA) (ITAM-0613);
- viii) Configuration Management (CM) (ITAM-0614);
- ix) Contingency Planning (CP) (ITAM-0615);
- x) Identification and Authentication (IA) (ITAM-0616);
- xi) Incident Response (IR) (ITAM-0617);
- xii) Maintenance (MA) (ITAM-0618);
- xiii) Media Protection (MP) (ITAM-0619);
- xiv) Physical and Environmental Protection (PE) (ITAM-0620);
- xv) Planning (PL) (ITAM-0621);
- xvi) Personnel Security (PS) (ITAM-0623);
- xvii) Risk Assessment (RA) (ITAM-0625);
- xviii) System and Services Acquisition (SA) (ITAM-0626);
- xix) System and Communications Protection (SC) (ITAM-0627); and
- xx) System and Information Integrity (SI) (ITAM-0628); and

b) Determine that the above action is not a project under the California Environmental Quality Act (CEQA) pursuant to CEQA Guidelines Sections 15378(b)(2) and 15378(b)(5) because it consists of government administrative activities, including general policy or procedure making, that will not result in direct or indirect physical changes in the environment.