

Attachment A

International Connectivity to County Assets Policy (ITAM-0575)

**COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL**

SUBJECT:	INTERNATIONAL CONNECTIVITY TO COUNTY TECHNOLOGY ASSETS POLICY	ITEM NUMBER:	ITAM-0575
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE 1 OF 4

I. Purpose

The purpose of this policy is to address the risks associated with connecting to County Technology Assets from outside the United States.

Connecting remotely to County Technology Assets and/or possession of County data on devices from outside of the United States poses risks that vary depending on the country or region being visited. Some countries present lower risks while others significantly greater risks. Risks related to countries and regions change from time to time, where a region considered low risk today may present high risks tomorrow.

Accordingly, it is important that all risks are evaluated and appropriate security measures are in place prior to County users remotely connecting to County Technology Assets when outside the United States.

II. Audience

The audience for this policy is all County employees, contractors, and Third Parties who access County Technology Assets who want and have a business need to access County Technology Assets when traveling outside the United States

III. Scope

This policy applies to all persons performing work for, on behalf of, and/or in support of the County with access to County Technology Assets or County data and who have a business need to access County Technology Assets when traveling outside the United States. This includes employees, independent contractors, consultants, temporary workers, and others performing work for, on behalf of, and/or in support of the County, including all personnel affiliated with such independent contractors and consultants, collectively referred to hereinafter as "Agents".

IV. Definitions

- o **County Technology Assets** – Hardware, software, applications, peripherals, services (including SaaS applications or otherwise).
- o **Disallowed List** – The list maintained by Central IT of high-risk countries within which connection to County Technology Assets or the possession of County data is prohibited.
- o **Device(s)** – Electronic devices capable of an internet connection, including, but not limited to, laptops, tablets, and smartphones.

**COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL**

SUBJECT:	INTERNATIONAL CONNECTIVITY TO COUNTY TECHNOLOGY ASSETS POLICY	ITEM NUMBER:	ITAM-0575
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE 2 OF 4

- Allowable Devices include:
 - County-managed **Trusted** Devices CONFIGURED by County departmental technology staff in accordance with applicable policies.
 - Non-County managed **Trusted** Devices
- Prohibited Devices include:
 - Everything else.
- **Third Party** – A supplier of goods or professional services which is independent of the customer.
- **Trusted Device** – A device operated in accordance with intended use that is independently verified by County IT to contain a fully patched, up-to-date operating system; fully patched, updated applications; and an updated anti-virus program (as applicable).

V. Policy

It is the Policy of the County of Santa Barbara that:

Connections to County Technology Assets and/or possession of County data on Devices outside the United States will only be allowed:

- For bona fide County business reasons;
- On a temporary case-by-case basis and only for the approved specified time frame;
- After obtaining approval, prior to travel, from Central IT/CISO or, in cases of appeal, from the Assistant County Executive Office;
- For individuals who have completed IT security training, including any supplemental training deemed necessary by the County CISO;
- In countries and regions that are not on the Disallowed List maintained by the County CISO/Central IT;
- Using Allowable Devices; and
- In compliance with all processes, procedures (e.g., sanitation of devices upon return from travel) and standards (e.g., encryption, multifactor authentication) promulgated by the County CISO/Central IT.

Connections to County Technology Assets and/or possession of County data on Devices while in any country on the Disallowed List is prohibited. Central IT will maintain the Disallowed List of known high-risk countries based upon research-based government and private sector data used by the Federal government in its Federal Risk and Authorization Management Program (FedRAMP®) to minimize security risks to agencies such as DOD and DHS in their use of modern cloud technologies. Countries

**COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL**

SUBJECT:	INTERNATIONAL CONNECTIVITY TO COUNTY TECHNOLOGY ASSETS POLICY	ITEM NUMBER:	ITAM-0575
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE 3 OF 4

that are in political turmoil or with governments capable of confiscating County Devices, data, or credentials will be included on the Disallowed List.

Connections to County Technology Assets may be terminated without notice during the travel period if deemed necessary by the County CISO or Central IT due to changes in the risk environment.

Connections to County Technology Assets by any other means, methods, or equipment not sanctioned by the County CISO/County IT are strictly prohibited.

Central IT, in collaboration with the County CISO and input from Departmental IT staff, are directed to establish and maintain procedures, subject to the IT Policy Committee's approval, to facilitate this policy.

Departments have the right to appeal decisions from the County CISO/Central IT to the County Executive Officer.

In the event of loss of a County Device or personal device which may have previously been used to connect to County Technology Assets, or which may contain County data, such loss must be reported by the custodian of such Device to such custodian's Departmental IT staff as soon as possible to facilitate appropriate security actions.

VI. Exceptions

Public Safety department personnel responding to emergent events where time is of the essence are exempt from obtaining advance approval from the CISO/Central IT for use of Allowable Devices during travel. However, such travel is to be reported to the CISO/Central IT as soon as practical, and all other aspects of this policy and related procedures are to be followed.

VII. Non-Compliance

County employees who fail to adhere to this policy may be subject to disciplinary action, up to and including termination in accordance with civil service rules. Agents who fail to adhere to this policy may face contractual penalties.

VIII. References and Sources

- 1) Applicable Rules, Laws, and Regulations
- 2) Related Policies:

**COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL**

SUBJECT:	INTERNATIONAL CONNECTIVITY TO COUNTY TECHNOLOGY ASSETS POLICY	ITEM NUMBER:	ITAM-0575
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE 4 OF 4

a) Acceptable Use Policy (ITAM-0550)

3) Referenced Documents:

4) Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	EITC Policy Committee	6/27/2022
1.0	EITC Approval	EITC Policy Committee	8/17/2022