ENTERPRISE COMPUTE ENVIRONMENT

Information Resource Responsibility Agreement (IRRA)

Welcome to the Enterprise Compute Environment (ECE) platform! This document explains how to use the ECE platforms, what's expected of you as an account holder, and how to onboard to our Public and Private Cloud Infrastructure-as-a-Service environments. Our Public Cloud options include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). We also offer a TAMU Private Cloud environment from various providers hosted on at the TAMU West Campus Data Center (WCDC).

After onboarding, Technology Services will bill your monthly costs to your provided FAMIS account. You'll have access to our cost management portal to monitor spending and create custom reports. Once you acknowledge the ECE requirements, we'll create your account and send access information and instructions.

For any questions or assistance with ECE, contact the ECE Management Team (ECE-MT) at enterprisecompute@tamu.edu.

ACCOUNT OWNER RESPONSIBILITIES

ECE Account Owners have responsibilities and roles related to acceptable use, fiduciary, security, and data protection. A general summary of these responsibilities follows.

ECE Account Owners may delegate these responsibilities to other individuals (stewards, managers, custodians) as outlined by **TAMU Security Control DC-2**. These delegations must be kept on file with the Management Team.

Acceptable Use

Use ECE only to conduct official business on behalf of your Texas A&M University System affiliated member. All ECE account users must abide by the Acceptable Use policy laid out in Texas A&M University (TAMU) **SAP 29.01.03.M0.02**.

Fiduciary

Account Owners are responsible for managing their ECE charges and confirming fund availability before using ECE resources. You must monitor their consumption using TAMU or other cloud tools, ideally monthly. Billing Alerts can notify them of cost thresholds or planned high usage. Cost Optimization meetings are encouraged to be had regularly and are available upon request.

Security Requirements

ECE Account Owners must classify their data using the TAMU **Data Classification Tool** upon onboarding, submitting the resulting report with any resource request. Owners managing **Confidential** or **Critical** data must also provide relevant Data Use Agreements (or similar documents) if contractually obligated to external entities, as these may require specific configuration changes.

All ECE tenants must participate in the **annual TAMU Risk Assessment** facilitated by Technology Services IT Security and Risk.

All **TAMU-System Security Controls** and applicable rules, regulations, standard administrative procedures, and the like, when using the environment must be followed by all who have access to the Platform.

Data Protection

During onboarding, you'll need to implement a data backup plan, to minimize the risk of data loss. The specific backup requirements depend on your account's business **impact level**. For accounts with a moderate or high impact rating, Texas A&M University's Controls Catalog CP-2 (**Contingency Planning**) requires a defined Recovery Time Objective (RTO) documented in a Business Impact Assessment (BIA).

Texas A&M University Security Control CM-3 (**Configuration Change Control**) mandates a consistent process for managing changes to information resources. If you have elevated permissions to independently manage your environment, you must coordinate your changes appropriately to comply with this control. Patching all compute resources within your environment is also your responsibility as the Account Owner.

Finally, as an ECE Account Owner, you agree to adhere to the **TAMU System Record Retention policy**. If you have specific data retention requirements that differ from this policy, please inform the ECE Management Team (ECE-MT) so we can ensure compliance.

MANAGEMENT TEAM RESPONSIBILITIES

Compliance of data and resources in ECE is a shared responsibility. ECE-MT, as **Data Custodian**, facilitates compliance monitoring and has privileged access to review events related to resource performance and security. Technology Services personnel may also take proactive actions to protect other TAMU resources in ECE and TAMU network. ECE-MT will maintain user data confidentiality and only disclose it to authorized university officials.

ECE uses the Technology Services Change Control process (per **TAMU Security Control CM-3**) and participates in weekly Change Advisory Board meetings. Account Owners will be notified of maintenance windows and changes affecting their accounts as approved by this process.

A Business Associate Agreement (BAA) covers all ECE environments with confidential data. Account Owners with confidential data may have additional responsibilities per the **TAMU and TAMU System Controls and Policies**. BAA changes will be communicated.

ECE-MT will apply custom tags to your environment during onboarding to aid management, performance monitoring, and cost visibility.

You will receive a PDF copy of this agreement via email.

UPDATES TO THIS AGREEMENT

This agreement may be updated from time to time. Account Owners are responsible for periodically reviewing this document for any changes. Notice of any updates will be communicated to Account Owners in advance via email. Continued use of the ECE platform following notification of changes constitutes acceptance of the updated agreement.