Science Managed Cloud Environment (SMCE)
User Agreement and Rules of Behavior

Introduction

The Computational and Information Sciences and Technology Office (CISTO – Code 606) at the NASA Goddard Space Flight Center (GSFC) provides a managed cloud environment using public cloud services specifically designed for collaborative science and application development. The Science Managed Cloud Environment (SMCE) is currently a FISMA-Low information technology environment using Amazon Web Services (AWS) based infrastructure for NASA funded researchers and collaborators. This environment is designed for the following:

- Provide public cloud access to NASA funded projects with team members both within and external to NASA;
- Perform research using emerging cloud computing capabilities without extensive start-up times;
- Access to innovative tools and methods from AWS to build cloud-native applications;
- Scalable computing and storage infrastructure.

The SMCE has a NASA Authorization to Operate (ATO) with reasonable controls that comply with relevant security requirements to guard the confidentiality, integrity, and availability of the work performed in the SMCE. This document provides information about the SMCE environment, security, roles and responsibilities, and user behavior. All Principal Investigators and System Administrators within the SMCE are required to acknowledge that they have read and will abide by this document once per year.

Roles and Responsibilities

SMCE Management Team: The SMCE Management Team provides overall project management, operational oversight, and security services for the managed environment.

SMCE Cloud Administrator (SMCE CloudAdmin): The SMCE has an operational staff of system administrators that are responsible for the overall configuration management and security of the managed environment, including any shared services, such as scanning and logging. Furthermore, the SMCE CloudAdmins are available to answer questions and trouble shoot problems as they may arise. Each project will have one or more accounts associated with the SMCE CloudAdmins that are included into the "SMCE-CloudAdmins" group and cannot be removed from the project.

Principal Investigator (PI): This is the NASA person responsible for managing the project within the SMCE and the users of the environment. The PI will have AWS console access and will be able to create user accounts. The PI is responsible for communications with the SMCE system administrators and management team, and also responsible for the associated AWS costs. The PI will be placed into the "SMCE-ProjectAdmins" group.

Project System Administrator (Project SysAdmin): Each project must define a system administrator that will be responsible for the patching and configuration management of the project's environment and applications. In the event of a security vulnerability, the project system administrator (and ultimately the PI) are responsible for mitigating the vulnerability. The Project System Administrators will be placed into the "SMCE-ProjectAdmins" group. A part of the on-boarding and security training will include general information about managing users and EC2 instances in the AWS Console.

Project Console User: Each project may also define general users that access AWS resources within the project. All Project Console Users must be placed within the "SMCE-ProjectPowerUsers" group, which will provide some limits on these user accounts; for example, general project users will not be able to create other user accounts (only the PI and the Project System Administrator can create accounts).

End User / Service User: Each project may provide certain users with access to their project's services, but without AWS console access. These users must adhere to the project and/or service requirements and are not required to abide by the terms of this User Agreement.

SMCE User: Any consumer of SMCE resources, to include the PI, Project Sysadmin, Project Console Users, and End/Service Users.

Authorization
Once a project is initiated, the PI and Project SysAdmins must receive their account authorization from the SMCE Information Systems Security Officer (ISSO). Project users (both NASA and non-NASA) may be created by the PI, Project SysAdmin, or a SMCE CloudAdmin once a signed user agreement has been provided for each individual. The PI and/or Project SysAdmin is responsible for providing the following information to the SMCE CloudAdmins for each user account to help with communications:

- Full Name
- Preferred User Identifier
- Organization
- Email
- Phone Number

In the event that a user is no longer authorized to access the project resources, the PI and/or the Project SysAdmins must remove the account and any related AWS permissions and notify the SMCE SysAdmins of this account removal. The SMCE CloudAdmins can support access removals if the project needs support to do this on their behalf.

Multi-Factor Authentication
For enhanced security, all SMCE users must authenticate to the AWS Identity and Access Management (IAM) repository using Multi-Factor Authentication (MFA), which employs something they know (their UserID/Password), and something they have (such as a hard or soft "token"). The SMCE implementation uses the Google Authenticator App, which sends a soft "token" to each user at the time of login.

The MFA requirement for SMCE also applies to the use of AWS API Keys, which can be used to provide automated script-based access to SMCE resources. Proper use of AWS API Keys will also require the use of Google Authenticator, which will issue a soft "token" to each user, and which will be required to generate a temporary session key at the time of each API Key use.

In the event that automated processes require access to the AWS API, an exception may be granted that will not require MFA for certain "service" accounts that are never used for interactive logins. All exceptions must be documented an exception with the ISSO.

API Key Usage
Use of AWS API Keys shall be minimized. These keys shall be treated as Controlled Unclassified Information (CUI) information and protected as such at all times. AWS API Keys shall never be uploaded to publicly available locations, as this could cause the entire SMCE environment to be severely compromised.

User Password and Key Expiration
All SMCE passwords and AWS API Keys must comply with NIST guidelines and shall be changed at least every 60 days (if not sooner). Any passwords or API Keys that are discovered to exceed this threshold will immediately be expired and will need to be changed prior to use. In addition, any user IDs that are inactive for > 60 days will also be expired. In all cases, a SMCE CloudAdmin will need to be contacted via support@nccs.nasa.gov in order to regain access to SMCE.

Data
SMCE has been categorized as a Federal Information Security Management Act (FISMA) "Low" system, which is only appropriate for the storage and processing of public data that is openly available. Uploading of classified, CUI, ITAR, or other sensitive data to the SMCE is not permitted. PIs are responsible for ensuring the data in use by their project is compliant with this requirement at all times.

Rules of Behavior
Users of the SMCE are responsible for using the managed cloud environment for NASA research and do so in a secure, ethical, and lawful manner. Users are responsible for all actions taken within their account and while the user account is open. As such, users must adhere to the following behaviors:

- Shall not share their account, passwords, or keys.
- Shall not import, use, or store any CUI, Classified, Export Administration Regulations (EAR), or International Traffic in Arms Regulation (ITAR) information.
- Shall not import, use, or store any fraudulent, harassing, or obscene information.
- Shall not divulge access information to any non-user of the project.
- Shall not purposefully engage in activities to harass another user, to deprive another user, to gain access to other information technology resources for which access has not be authorized, to degrade the performance of a system or service, or to circumvent security measures.
- Shall report any weakness in the security of the environment to the SMCE management, security, and system administration team members, and shall disclose any incident of possible unauthorized use.
- Shall not use social media platforms as a vehicle for sharing SMCE project information and shall not post organizational information about SMCE on social media or other public websites.

Configuration Management
SMCE will provide custom Amazon Machine Instances (AMI), which will be maintained within the configuration and security management services of the SMCE environment. The SMCE team will ensure all custom AMIs are maintained per NIST guidelines and will make these AMIs available to PI and systems administrators for use in the creation of all new instances.
PIs will ensure that all SMCE instances are not altered significantly from the established custom AMIs without prior permission from the SMCE team. Examples of settings that shall not be altered include the following:

- Systems Manager agents installed on all EC2 instances
- Center for Internet Security (CIS) benchmark settings
- NIST-compliant patch management schedules
- Notification to SMCE Security Team of unsuccessful login attempts
- Use of a NASA-approved system use notice (at time of logon)
- Adequate storage for audit records
- Storage of audit failure alerts
- Use of AWS CloudTrail to monitor activity by all SMCE users

Information System Backups
All backups and disaster recovery are the responsibility of the PI and system administrator for each project. PIs must have a backup strategy for all data stored within their individual project resources and will ensure that regular backups are conducted.

Incident Response
In the unlikely event of a security incident, SMCE users will be required to fully cooperate with the SMCE Management, System Administrators, and Security team immediately in order to effectively respond to an incident and to perform any necessary remediation activities. If an SMCE User thinks their EC2 instances or data have been compromised, they should immediately do the following:

1) Stop the affected EC2 instances (but do not terminate them). Terminating an EC2 instance will delete any system logs that will be necessary for post-incident forensic activities.
2) Contact the SMCE System Administration via support@nccs.nasa.gov or via phone if an immediate response is not received. Specific information about how an SMCE user can effectively respond to security incidents is included in the annual SMCE General Security Training.

Vulnerability Management
PI and Project SysAdmins will receive weekly Inspector vulnerability reports and will be required to collaborate with the ISSO and CloudAdmin team to remediate all vulnerabilities according to the following schedule:

- Expedited (SOC MAR): 7 Calendar Days
- Critical: 15 calendar days
- High: 30 calendar days
- Medium: 30 calendar days
- Low: 60 calendar days

These updates will include both Operating System patches and application updates, the details of which will be included in custom weekly reports delivered to all PIs and Project SysAdmins with vulnerable EC2 instances. Additional information about the Common Vulnerabilities and Exposures (CVE) presented in the custom weekly Inspector reports is available in the AWS Inspector v2 Dashboard.

Blocklist Processing
If an EC2 instance for an SMCE project does not have the Systems Manager (SSM) agent installed or has not been patched within the required timeframe as noted in the Vulnerability Management section

above, the PI and Project SysAdmin will be notified of a pending action to place this instance on a blocklist. If the required actions to remediate the vulnerabilities are not completed within the timeframes specified above, the affected EC2 instance will be temporarily shut down, with all access blocked. As necessary, the SMCE ISSO and CloudAdmin team will distribute a blocklist at least 7 days prior to any instances being blocked to provide advance warning of pending blocklist actions.

Security Training
Annually, all users who have access to the AWS console must complete the SMCE General Security training, and Project SysAdmins must also complete the SMCE Elevated Privileges Security Training, both of which are available at the following link after authenticating to the AWS Console:

https://s3.console.aws.amazon.com/s3/buckets/smce-training/?region=us-east-1

For all NASA credentialed users, the NASA security training requirements still apply. In addition, all Project SysAdmins are strongly encouraged to take the NASA Elevated Privileges training (or equivalent within their organization), prior to being provided heightened privileges for cloud resources (e.g., root, administrator, power user, etc.). Agreement to these rules of behavior imply that the user has taken all requisite security training within their respective organization.

Community of Practice (CoP) Meetings
SMCE Community of Practice (CoP) meetings will be held on a regular basis for the purpose of providing SMCE specific information about operational capabilities and security while also creating an opportunity to share specific AWS implementations that could benefit the SMCE user community. Case studies and success stories for selected SMCE projects will be featured, which will serve to promote collaboration between all SMCE users, to include PIs, Project SysAdmins, and console users.

Attestation
This document describes the user behavior and security-related responsibilities for each SMCE user, which will serve to ensure the security of all SMCE resources. By downloading and reading the SMCE Security Training materials (at the URL shown in the Security Training section above), and reading and signing this SMCE User Agreement, this provides an attestation that you, as an SMCE user, will abide by the guidelines in these security documents, and that failure to do so may result in termination of your access to the SMCE environment.

SMCE Role:

[Please Select]

_____

Digital Signature/Date:

_____