PURPOSE: To establish a consistent policy and procedure at the Virginia Information Technologies Agency (VITA) to control access to the VITA Customer Account Support Tool (VCAST).

SCOPE: All VITA employees and approved Business Partners requesting and having access to VCAST. This system is considered sensitive with respect of confidentiality, integrity, and availability.

ABBREVIATIONS:

- COV – Commonwealth of Virginia
- CRM – Customer Relationship Management
- CSRM – Commonwealth Security and Risk Management Directorate
- VCAST- VITA Customer Account Support Tool
- VCCC - VITA Customer Care Center
- VITA - Virginia Information Technologies Agency

DEFINITIONS:

- VCAST (VITA Customer Account Support Tool) – an application based on the Microsoft Dynamics CRM commercial off-the-shelf (COTS) package that has been configured to be used to track information related to VITA accounts and contact interactions.

- VCAST Administrators – VITA employees responsible for set-up, configuration, development and maintenance of the VCAST system.

- VCAST Support – VITA employees responsible for providing support to the VCAST Users, performing quality assurance (QA) of all bug fixes and new development, and providing Administrative Support to the VCAST Administrators in the area of User Account set-up and maintenance.

- VCAST User - all VITA employees and approved Business Partners who have access to VCAST.

- VCAST Business Unit – one or more divisions, departments or functional groups within VITA using VCAST that may or may not align with organizational units. Business Units are directly tied into Security Roles and Levels of Access to records. Each VCAST user can belong to one, and only one, Business Unit.

- Organizational Unit – any organizational structure within VITA.

- VCAST Data – data that resides in the VCAST system.

- VCAST Entity - anything about which information can be stored (e.g., a contact, account or case). Each entity and its related data will have a business owner.

- VCAST Form - the user interface that appears for viewing and data entry when opening a specific record (such as, for account, contact, or case.)

- VCAST Case - a customer service event, issue or problem that requires follow up within VITA and/or its partners for resolution. A VCAST Case does not replace a VCCC ticket. Generally, a Case will include multiple contacts and multiple activities. For example, a Customer Account Manager (CAM) may open a Case to follow up with billing and inventory on a customer billing issue.

- VCAST Data Owner – a VCAST user who is identified to make decisions regarding the use of data and assist with ensuring the data is accurate.

- VCAST Private Case – a VCAST case that has been designated as private by an authorized user. A private case and its associated components can be accessed only by those employees and approved Business Partners specifically authorized by the private case owner. Every private case will have a parent case that is not private. All activities and Notes associated with a private case are also deemed private and thus accessible only by the private case owner and those employees and approved Business Partners specifically authorized by the private case owner.

- VITA SharePoint Site - a collection of pages, lists, libraries and related settings that are used by VITA in day to day business.

- SharePoint List - a container of information or data structure organized in two dimensions, rows and columns. Each row represents an individual record and each column represents a specific attribute value of that record.

- Business Owners – VCAST Users with decision making authority (and often times higher privileges) for the items they own. VCAST uses the concept of ownership to control data access to entities, records, data elements, and forms. A business owner can be a system user.

- Case Owner - a VCAST User responsible for ensuring the Case is managed through closure. A VCAST case can be owned by any VCAST system user or team. Cases may be closed / resolved only by users who have ownership rights to a specific case. A Private Case may be owned only by those authorized to own private cases. The Case Owner is responsible for determining the sensitivity of data contained

in the Case as defined in this policy. If the data is classified as sensitive, the Case Owner is responsible for ensuring that data is protected in a Private Case.

- CRM Program Owner – the person designated to lead and facilitate development and adoption of a VITA-wide CRM strategy including specific goals, objectives and performance measures and who is responsible for approving all VCAST access requests.

- CRM Program Manager – the person designated to manage the development, implementation and adoption of a VITA-wide CRM strategy including specific goals, objects and performance measures

STATEMENT OF POLICY:

VCAST provides a centralized location for VITA employees and approved Business Partners to access customer-related account, contact, and case information using an internet connection and COV credentials.

STATEMENT OF PROCEDURE:

VCAST Access Management Overview

The CRM Program Owner or his/her designee is responsible for approving all VCAST access requests.

Managers and supervisors are required to review the VCAST Business Unit assignment and Security Role assignments of their employees and approved Business Partners on an annual basis, when an automated report is available.

VCAST Administrators will have a list of overall VCAST access types, specific entity and form owners, as well as data owners. All access requests will be reviewed by the CRM Program Owner or his/her designee, CRM Program Manager or his/her designee and the VCAST Administrator before granting access.

VCAST links to LAN. SharePoint documents, folders and sites are managed outside of VCAST. The respective LAN and SharePoint business units and owners are responsible for managing access to those documents, folders and sites.

Authentication

Authentication will be performed by Windows Authentication on the COV network. Users can manage their own passwords based on guidelines supplied at https://esupport.virginia.gov/.

Access Request Process

See Access Request workflow in Appendix B: VCAST Access Request Process.

Private Case Designee Authorization

Private cases may be created and accessed by the executive team and their authorized designees. The process to add an authorized designee is found in Appendix B: VCAST Access Request Process.

Sensitive data
Sensitive data is defined in the ITRM Glossary as –

"Any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled."

For the purpose of this policy, the sensitive data definition above is extended to include data which:

- Is generally accepted as being non-public or confidential information, from both a personal or business perspective.
- Includes VITA internal documents or working papers that should not be shared with external entities (this could include documents subject to the Freedom of Information Act (FOIA)).
- Is a well-established sensitive data type, such as personally identifiable information (PII) or account numbers.

Any questions concerning the sensitivity of data should be addressed with CSRM prior to publishing the data to VCAST. The access, storage, processing and removal of Sensitive Data must comply in all instances with COV ITRM Security Policies found at this link:
http://www.vita.virginia.gov/library/default.aspx?id=537

Sensitive data must not be kept within the core Account, Contact, Note or Case records unless it is protected in a private case.

- Sensitive data may be stored outside of VCAST (e.g., Shared Drives) where it is protected in accordance with the COV ITRM security standard. VCAST may contain a reference (url) to the sensitive data folder.
- If data within VCAST becomes sensitive, the data will either be removed from VCAST or protected in a private case by an authorized user.

Access Types/Roles
Security privileges are based on business functionality and data needs. Each security role has the following possible privileges:

- Create (Add new record)
- View
- Edit
- Delete
- Append (an example is to open a case, and from within the Case create a Note that automatically becomes a part of the Case record)

- Append To (an example is to create a new Task record and set it regarding a Case record. The task is now appended to the case and becomes a part of the Case record.
- Assign (Change ownership of the record)

The individual roles available within VCAST are:

- **VITA Audit** – the VITA audit security role. This role requires and adds to the VITA Base Access security role and does not stand alone.

  The privileges included in this role:

  - Ability to view all private cases.
  - Ability to view all private activities.

- **VITA Base Access** - the base role for all VITA VCAST users.

  With the privilege of VCAST access, users shall remember that any data, notes, comments, records, documents that are input into VCAST may be available to the public and/or be made available through FOIA. Therefore responsible and diligent discretion should be considered during a user's access and input into VCAST.

  Base Access privileges include the following level of authorization for non-private cases except where private cases are explicitly indicated:

  - Account Records –
    - The ability to view all the account records within VCAST (e.g., Agencies, Local Govt, Suppliers)
    - The ability to edit all unlocked fields on all account records within VCAST.
    - The ability to assign and share any account record owned by the user or by anyone within the user's Business Unit.
    - The ability to append and append to any account record within VCAST.
  - Activity Records (include Tasks, Appointments, Emails, Phone Calls, Letters, Faxes) –
    - The ability to create activities that can be viewed by any VCAST user.
    - The ability to view all activities owned by any VCAST user.
    - The ability to edit, assign, append and share any activities owned by the user or by anyone within the user's Business Unit.
    - The ability to append to any activity owned by any VCAST user.

        - The ability to view, edit, delete, append, append to, assign and share any private activities owned by the VCAST user
    - Announcements -
        - The ability to view all announcements within VCAST
    - Connection records
        - The ability to create connections that can be viewed by anyone within the organization.
        - The ability to view, append and append to all connections and connection roles owned by anyone within VCAST
        - The ability to delete any connection owned by the user
        - The ability to edit or share any connection owned by the user or by anyone within the user's Business Unit
    - Contact Records
        - The ability to create contact records that can be viewed by anyone within the organization.
        - The ability to view all the contact records within VCAST (e.g., State Employees, Contractors, Local Govt contacts, Supplier Contacts)
        - The ability to edit all unlocked fields on all contact records within VCAST.
        - The ability to assign and share any contact record owned by the user or by anyone within the user's Business Unit.
        - The ability to append and append to any contact record within VCAST.
    - Email Templates
        - The ability to view all VCAST system email templates.
        - The ability to create, edit, delete, assign, share, append or append to email templates owned by the VCAST User.
    - Note Records
        - The ability to create notes that can be viewed by all VCAST Users.
        - The ability to view all within VCAST.
        - The ability to edit or share any note owned by the VCAST User or by anyone within the user's Business Unit
        - The ability to append or append to any note within VCAST.
        - The ability to delete a note owned by the VCAST User.
        - The ability to view, edit or delete any private note owned by the VCAST user.
    - Reports
        - The ability to create reports that are only viewed by the owning VCAST User.

        - The ability to view, edit, delete, append, append to, assign or share any reports owned by the VCAST User.
    - Personal Views
        - The ability to create views that are only available to the owning VCAST User.
        - The ability to view, edit, delete, assign or share any views owned by the VCAST User.
    - Personal Charts
        - The ability to create charts that are only viewed by the owning VCAST User.
        - The ability to view, edit, delete, assign or share any charts owned by the VCAST User.
    - Audit Data
        - The ability to view audit history and summary data for audited records.
    - Dashboards
        - The ability to create dashboards that are available only to the owning VCAST User.
        - The ability to view, edit, delete, assign or share any dashboards owned by the VCAST User.
    - Articles
        - The ability to view all VCAST articles.
    - Case Records
        - The ability to create cases that can be viewed by all VCAST Users.
        - The ability to view, append, append to all cases within VCAST.
        - The ability to edit, assign or share any cases owned by the VCAST User or by other VCAST Users within the user's Business Unit.
        - The ability to view, edit, delete, assign or share any private cases owned by the VCAST user.
    - COV Role Assignment Records
        - The ability to view all COV Role, VITA Role Designation and COV Role Assignment records within VCAST.
    - Business Management Privileges
        - The ability to export all data within VCAST into Excel
        - The ability to view records sync'd to Outlook when offline.
        - The ability to print any record user has authorization to view within VCAST
        - The ability to sync Outlook and VCAST records owned or shared with the user

- **VITA Maintain Accounts** – An additional security role allowing authorized users the ability to activate and deactivate account records. The VITA Maintain Accounts security role requires and

adds to the VITA Base Access security role and does not stand-alone.

Additional privileges include:

- The ability to activate and deactivate VCAST customer account records.

- **VITA COV Role Assignments -** An additional security role allowing the ability to manage the COV Role Assignments. The VITA COV Role Assignments security role requires and adds to the VITA Base Access security role and does not stand-alone.

  Additional privileges include:

  - COV Role records
    - The ability to edit, append, append to all COV Role Records owned by any VCAST User.
  - COV Role Assignment
    - The ability to create, edit or delete, append, append to all COV Role Assignment Records owned by any VCAST User.
  - VITA Role Designation
    - The ability to create or edit all VITA Role Designation Records owned by any VCAST User.

- **VITA Private Data Enhanced Functionality** – An additional security role allowing the ability to create private cases and private actitivies. The VITA Private Data Enhanced Functionality security role requires and adds to the VITA Base Access security role and does not stand alone.

  The privileges included in this role:

  - Ability to create private cases and private activities associated with private cases.

- **VITA Service Offerings – Relate Accounts** – An additional security role allowing authorized VITA VCAST Users the ability to map the relationship between discreet VITA Services and the Accounts which utilize those services.

- **VITA Service Offerings – Maintain Service Information** – An additional security role allowing authorized VITA VCAST Users the ability to add, modify and/or retire the discreet VITA Services.

- **VITA Data Steward -** An additional security role allowing authorized VITA VCAST Users the ability to edit locked down fields on account and contact records owned by the user or other users within the user's business unit. The VITA Data Steward security role requires and adds to the VITA Base Access security role and does not stand alone.

  - **Additional privilege**s include:

- The ability to change data in the following fields on the Data Steward Form for Customer Accounts:
  - Account Name
  - Account Type
  - Account Classification
  - Account#
  - Acronym
  - Segment
  - Mandated for ITP Services
  - Receives ITP Services
  - Parent Account
  - Secretariat Name
  - Branch
  - Agency #
  - Spend Fiscal Year
  - Budget Fiscal Year
  - Average (Spend+Budget)/2
  - Rank
  - FIPS Code
  - Planning District Number
  - Customer Site Code
  - Inventory Billing Roll-Up Account
  - Comprehensive Services Billing Indicator
  - Computer Services Billing Indicator
  - Telco Billing Indicator
  - Primary Email
- The ability to change data in the following fields on the Data Steward form for Contacts (only for those Contact records that are **not** sourced from a feed):
  - Employment Type
  - Parent Account
  - Contact Classification
  - Last Name
  - Approval for System Feeds
  - Department
  - Working Title
  - Manager

- **System Administrator -** An out of box security role that is not customizable and is designed only for developers. The System Administrator security role provides full access to everything within the VCAST tenant, including full read/edit/delete access to all records within VCAST.

  Additional privileges include the ability to:
  - Adjust system settings
  - Enable/disable system reports/charts/views
  - Import solutions (migrate code) and publish
  - Create/edit business unitsThe ability to define relationships
  - Manage web resources
  - Import data
  - Create duplication rules and set them to execute
  - Adjust user settings

- Add and manage user accounts
- Act on behalf of another user if requested
- Create templates
- Import jobs
- Manage option sets

Business Function Table

The following table represents an overview of the Business Functions supported in the current release, and the security roles necessary to support each function.

Business Function	Security Roles
Access VCAST with no elevated privileges (default Security Role for all VITA VCAST users)	VITA Base Access
Account maintenance (currently limited to Activating and Deactivating Account records)	VITA Base Access VITA Maintain Accounts
Managing COV Role Assignments (the relationship of a Contact to an Account with a specific COV Role)	VITA Base Access VITA COV Role Assignments
VCAST System Administrator (total access to the entire tenant. This includes the ability to manage VCAST user accounts, administer the VCAST application, perform development tasks, customizations, system settings, manage solution files, create/manage security roles, import data, bulk record updates, manage duplicate rules, merge records, create/maintain reports, create/maintain web resources, create plug-ins, create/maintain templates, create/maintain business units and teams, create/manage system jobs, configure and manage sharepoint document locations and set up/maintain the product/service catalog structure.)	System Administrator
Maintenance of the services used by Accounts	VITA Base Access VITA Service Offerings – Relate Accounts
Maintenance of the service information	VITA Base Access VITA Service Offerings – Maintain Service Information

Changes

Changes to existing User Accounts would follow the VCAST Access Request process (see Appendix B: VCAST Access Request Process).

Deactivating User Accounts

- VCAST System Administrators receive Separation Notifications from Human Resources. When the VCAST System Administrators

receive the Separation Notification for an individual, they disable the user account from all VCAST environments.

Periodic Review of User Accounts

All assigned roles will be reviewed on the following schedule:

- Quarterly:
  - System Administrator role – reviewed by the Director of Cross Functional Support, CRM Program Manager, Security and Audit;
  - VITA Private Data Enhanced Functionality – reviewed by CRM Program Owner, CRM Program Manager and applicable Managers and supervisors
  - VITA Audit – reviewed by CRM Program Owner and CRM Program Manager
  - VITA Data Steward – reviewed by CRM Program Owner, CRM Program Manager and applicable Managers and Supervisors
- Annually: All other roles - Reviewed by CRM Program Owner, CRM Program Manager and applicable Managers and supervisors.

If a supervisor or manager does not respond within 30 calendar days to the initial request for review of role assignments, the applicable role assignments will be deactivated, which may result in the revocation of access to VCAST entirely.

The Chief Information Officer's access shall be reviewed by the Chief Information Security Officer.

VCAST Usage

- VCAST is a collaborative work tool that enables sharing of information and collaboration. VCAST is not a records management tool.
- Users must adhere to Security Policies and Procedures and to Records Management Policies and Procedures. VCAST may be be used to track tasks associated with in process, draft, and collaboration documents but should not be used to store those documents. Draft documents may be stored on SharePoint or the LAN. Official records must be stored on shared drives.
- While VCAST allows for storage of key information and links to other document repositories and collaborative tools, it is not an agency wide document storage repository.
- All VCAST users must have signed the Internet Usage Agreement, which is part of the new-hire on boarding process. Site usage and content is subject to the Internet Usage Policy, as well as all VITA Policy and Procedures referenced below.
- Business Owners are accountable for compliance with the current COV ITRM Information Security Standard, the COV ITRM IT Security Audit Standard; and, all standards and/or regulations controlling the storage, handling and dissemination of sensitive data.
- VCAST users with access to private case or activity data are responsible for ensuring that data is only shared with authorized users or teams and that they comply with all standards and/or

regulations controlling the storage, handling and dissemination of sensitive data.

- VCAST's system owner will advise and educate Users and Business Owners on the roles and responsibilities in using VCAST where sensitive data is stored and used.
- It is required that the owner of VCAST overall, VCAST Form and Workflow establish documented procedures for Logical Access Controls, Technical Controls and Account Management for site data that may require additional security such as data that is deemed sensitive (ref. IT System and Data Sensitivity Classification Policy and Procedure and Logical System Access Control Policy). This document serves as the logical access control documentation for VCAST.
- All VITA VCAST information and data are subject to review by VITA Audit. Compliance with this policy requires members of the VITA Audit active directory groups to have the VITA Audit security role.
- Specific data elements (tables,fields and attributes) used in VCAST will each have a business owner. If data is pulled from outside sources such as PMIS, PAA or PeopleSoft, CRM Program Owners and data owners will have to approve any changes, usage or updates before the change is made in VCAST. Data elements that are sourced from external systems (such as PMIS, PAA, PeopleSoft) cannot be updated by VCAST Users within the VCAST system.
- VCAST Administrators will monitor VCAST usage to help manage the health of VCAST.
- Related VCAST LAN and SharePoint Site Owners must document processes for managing logical access and perform periodic reviews of access to sites where required by COV IT Security Standard and VITA policy and procedures.

Content/Enhancements

- Directors or Managers must authorize their staff to access VCAST, the data and information stored within VCAST as well as any requests for VCAST data, entity, form, case or VCAST overall updates or changes.
- All requests for enhancements should be submitted to the VCCC. All requests must be approved by the VCAST Program Manager and the VCAST Change Control Team before being evaluated by the VCAST technical team.
- Development must be completed in the development environment and tested in the test environment prior to placing a change in the production environment. Business owners must participate in testing and approval of moves into production.
- VCAST links to LAN and SharePoint documents and sites are managed outside of VCAST. The respective LAN and SharePoint business units and owners own and manage the content and are solely responsible for all information on their LAN or SharePoint sites.

ASSOCIATED POLICY/ PROCEDURE: VITA Records Management

DHRM Policy 1.75 - Use of Electronic Communications And Social Media
ITRM Standard SEC501-08 Information Security Standard
ITRM Standard SEC502-02.2 Information Technology Security Audit Standard
IT System and Data Sensitivity Classification Policy and Procedure (available at VITAweb > Resources > Policies & Procedures)
Logical System Access Control Policy and Procedure (available at VITAweb > Resources > Policies & Procedures)

AUTHORITY REFERENCE: *Code of Virginia, §§ 2.2-2005 – 2.2-2032*
(Creation of the Virginia Information Technologies Agency; "VITA"; Appointment of Chief Information Officer (CIO))

OTHER REFERENCE: None

Version History		
Version	Date	Change Summary
1	11/5/13	Original document
2.0	10/31/14	Modified role review schedule; changed references to organizational units to conform to new organizational structure
2.1	10/13/10	Administrarive change

Appendix A: System Inventory

system name	VITA Customer Account Support Tool (VCAST)
system type	Browser/Client based
system owner	CRM Program Owner: Judy Marchand Hampton CRM Program Owner Designee: Susan McCleary CRM Program Manager: Susan McCleary CRM Program Manager Designee: Mary Fain
system's physical location	CESC Data Center
date of last update	November 5, 2013
Information submitted by	Mary Fain

Appendix B: VCAST Access Request Process