RSA SecurID Tokens Service Level Agreement (SLA)

1. Agreement

This Agreement defines RSA SecurID services provided to a Customer. Service definitions include responsibilities, hours, availability, support levels, and restrictions on support.

This Service Agreement (this Agreement) is effective September 30, 2012 between Vanderbilt Information Technology Services (ITS) (hereafter referred to as Service Provider) and Departments that have purchased this service (hereafter referred to as Customer) and establishes a commitment for providing RSA SecurID service (Service) as detailed in this Agreement. This document clarifies both parties’ responsibilities and procedures to ensure Customer needs are met in a timely manner.

1.1 Services Provided

The following service(s) are provided to the Customer by this agreement.

- The Customer will be provided with administrative access the RSA SecurID environment
- Tier 3 support as defined in section 3.5

2.1 Service Objectives

Processes outlined herein are in effect during normal service hours 08:00 AM - 04:30 PM Monday through Friday. Incident response is worked 24 hours a day, seven days a week.

The standard maintenance window is on Sunday from 12:01 AM – 4:00 AM. Most planned outages will occur during this window. Any other planned outages will be scheduled during the nights and weekends following consultation with Customers.

The RSA SecurID availability goal is 99.8% during the defined service hours, excluding scheduled maintenance downtime or disasters outside of the Service Provider’s control.

2.2.1 Requesting Service, Service Calls and Incident Reporting

2.2.1.1 Incident Management and Service Goals

The Service Provider’s designate or other knowledgeable staff member will respond by email or telephone to the Customer’s incident within:
- 4 hours for issues classified as urgent.
- 1 business day for issues classified as normal priority, service request, or business inquiry.

2.2.1.2 Service Categories

<table>
<thead>
<tr>
<th>Impact</th>
<th>Categories</th>
<th>Escalation and Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgent</td>
<td>Security Console is not reachable, Self-Service is not reachable, no users are able to authenticate with RSA</td>
<td>Contact VUMC HelpDesk @ 343-4357</td>
</tr>
<tr>
<td>Service Request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Normal Priority</td>
<td>User permission issues, anomalous system behavior or system problem that does not prevent work on the system.</td>
<td>Contact VUMC HelpDesk @ 343-4357</td>
</tr>
<tr>
<td>Service Request</td>
<td>Routine request for Maintenance, request for seed token upload.</td>
<td>Contact VUMC HelpDesk @ 343-4357</td>
</tr>
<tr>
<td>Business Inquiry</td>
<td>A question regarding a change to the contracted service.</td>
<td>Contact your Service Delivery Manager</td>
</tr>
</tbody>
</table>

**2.2.1.3 Service Acquisition**

The Service Provider agrees to fulfill requests for additional RSA SecurID services for existing Customers.

Acquire new service by contacting your ITS Service Delivery Manager.

**2.2.1.4 Service Availability**

The Service Provider will make the service available 24 hours per day, all days of the year, with the exception of necessary planned interruptions for service, upgrades, and reconfiguration. The Service Provider will minimize the number and duration of these interruptions. The Service Provider will attempt to coordinate with all affected Customers to schedule the interruptions for times least disruptive to the Customers. The Service Provider will, except in cases of great urgency, provide the Customer with at least 3 business days prior notice of the interruption.

All Customer requests for service and service calls, as well as reporting of urgent incidents, should go through the VUMC HelpDesk at 343-4357.

**2.2.2 Exclusions**

The Service Provider cannot guarantee timeframes for the following situations:

- issues that are referred to a third party service provider
- systems in a disaster recovery state
- Issues that involve troubleshooting the operating system, applications, or content of systems attached to the RSA SecurID service.

**2.2.3 Escalation Procedures**

During normal business hours, the Customer should contact the VUMC HelpDesk for all urgent and non-urgent incidents. After regular business hours, for urgent issues the Customer should contact the Network Operation Center (NOC). If the situation is not responded to in a reasonable amount of time, the Customer should contact the NOC manager. If still unsatisfied with the response, the Customer should contact their Service Delivery Manager (SDM).
2.2.4 Outage Notifications

The Service Provider will communicate planned service outages to affected Customers. Depending on the breadth and impact of the outage, notification may be by phone call or by email. Notification will occur per contact information provided by the Customer.

2.2.4.1 Planned Outages

When possible, the Service Provider will communicate planned outages to Customers by phone call or by email at least 3 business days before the outage. If a planned outage becomes necessary in less than 3 days, the Service Provider will communicate soon after the outage necessity is determined.

2.2.4.2 Unplanned Outages

The Service Provider will communicate unplanned outages as time permits, to the first available Customer contact by phone (or, if unavailable, email) within two hours of the outage.

2.2.5 Scheduled Maintenance

To meet specified service availability and service level objective, regularly scheduled maintenance is necessary. When possible, maintenance will be performed from 12:01 a.m. to 4 a.m. However, much Data Center maintenance must occur during normal business hours. This work usually does not cause a Customer outage.

2.2.6 Constraints

The Service Provider contacts Customers using the data in our contact database. The Service Provider will attempt to contact one person, trying the site owner first and, if that person is unavailable, the alternate contact. The Customer must notify the Service Provider when a contact changes, provide a new contact person, and provide contact information. The Service Provider is not responsible if the Customer fails to update contact information.

2.2.7 Backup and Recovery

Customers are responsible for the backup and recovery of data on the Managed Storage. The Service Provider is not responsible for the Customer’s failure to implement a working backup and recovery plan. Each Customer is responsible for developing, implementing, testing and maintaining a Business Continuity Plan.

3. Responsibilities

This Service Level Agreement (SLA) between Customer and the Service Provider establishes a commitment for RSA SecurID as detailed in this Agreement.

3.1 Scope

The following services are provided to the Customer by this agreement.

- The Customer will be provided with the tools necessary to implement a new RSA SecurID instance. This includes guidance provided by their Service Delivery Manager throughout the implementation process and coordination with the Systems Access Management (SAM) team.
- The Customer will be provided with Tier 3 support by Service Provider as defined in Section 3.5.
- The Customer will be provided with services to load token seed records into existing security domains.
- The Service Provider will monitor the RSA SecurID service for availability as defined in Section 2.2.1.4.
- The Service Provider will communicate outages affecting the service to the contacts provided.
The following services are not provided under this Agreement:

- Installation or configuration of agents
- Tier 1 support as defined in Section 3.5.
- Tier 2 support as defined in Section 3.5.
- Administration of Security Domains and access to those Security Domains
- Administration of users or tokens
- Management or support of AD/LDAP authentication

3.2 Customers

RSA SecurID administration can be completed by Vanderbilt Staff only. RSA SecurID authentication can be used by any individual deemed appropriate, as defined by the application requirements.

3.3 Objectives

The primary goal of this Agreement is to obtain mutual agreement that the proper procedures, requirements, and service levels are in place to provide consistent service support and delivery to the Customer by the Service Provider.

The objectives of this agreement are to:

- Clarify service ownership, accountability, roles and/or responsibilities
- Present a clear, concise and measurable description of the services offered to the Customer
- Match perceptions of expected service offerings with actual service support and delivery.

3.4 Service Level Reviews

This agreement will be reviewed at an interval no greater than one year by the Service Provider.

3.5 Service Requirements

The Service Provider will

- Maintain appropriately trained staff
- Communicate in writing issues regarding service levels, change management, etc.
- Meet response and resolution times
- Maintain hardware within standard life-cycle
- Patch software as recommended by vendor

The Customer will

- Adhere to the Electronic Communications Policy [HR-025]
- Adhere to the support table below for their end-user support:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Categories</th>
<th>Escalation and Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 3</td>
<td>Security Console is not reachable, Self-Service is not reachable, no users are able to authenticate with RSA Tokens.</td>
<td>Contact VUMC HelpDesk @ 343-4357</td>
</tr>
<tr>
<td>Tier 2</td>
<td>User permission issues, token issues not resolved with Tier 1</td>
<td>End-user will contact Customer appointed administrator, Customer</td>
</tr>
</tbody>
</table>
The Customer should

- Implement internal disaster recovery planning for this service.

### 3.6 Agreement Changes and the Dispute Resolution Process

Customers wishing to amend this agreement should contact the Service Provider. Requests for changes to this agreement will generally follow the flowchart below.

<table>
<thead>
<tr>
<th>Tier 1</th>
<th>Request for tokens, assistance with pin reset, self-service access, general training on usage of token</th>
<th>End-user will contact Customer appointed administrator</th>
<th>administrator to escalate issues to SAM Team via VUMC HelpDesk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Change and Dispute Resolution Process

1. Customer proposes change to Service Delivery Manager

2. Service provider reviews proposed change for approval

3. Approved? (Yes/No)
   - Yes: Make required changes to documentation
   - No: Customer notified; process ends.

4. Customer or service provider implements change.

5. End

Service Level Agreement Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Person(s) Making Changes</th>
<th>Summary of Changes</th>
<th>Version Number</th>
</tr>
</thead>
</table>

[Publish Date] 6