

# **RAD Use Policy**

## **Remote Access Device Acceptable Use Policy**

### **Document Purpose**

Many agencies are considering the use of personal phones and other technology devices as a means to cut costs and/or provide their employees access to productivity tools available on smart devices. This document is intended to help those agencies and their staff make informed decisions about and set realistic expectations for the use of personally owned remote access devices or RAD's. RAD's have the capability to connect to the State's email system without the use of Citrix. The State email system includes email, contacts and calendar but does not include any of the network drives. Different types of RAD's include Smartphones, like BlackBerry, iPhones and Androids; mobile computing devices like iPods, iPads, and notebooks; as well as other non-state computers such as public access terminals located in libraries, schools and airports or any other email capable computing device.

### **Background**

There are many technical, legal, and regulatory issues that can have bearing on the use of personally owned RAD's for State business. Decisions on how to address these issues are best made by the agency for which an employee works. This document is intended to provide a base-line set of legal and technological expectations that will tend to apply equally across all State government. This can serve as the starting point for cost/benefit determinations. As part of that cost/benefit determination each agency is advised to examine its own audit and data security needs to accurately determine the business value and risks of allowing employees to use personal devices to connect to the State's email system. It is our hope that this document will provide a solid starting place to make that determination.

#### **1. Access Requests**

- a. Upon direction by an agency, BIT will activate or de-activate RAD access for individual or groups of users.

#### **2. Connectivity Considerations**

- a. Although BIT provides an industry standard email interface for use by RADs known as ActiveSync, each manufacturer will make use of that interface in the manner they find most effective. If a particular manufacturer's device will not work properly when accessing the interface provided, BIT can provide interface details to the service provider to help them determine whether the device they support is working correctly. We recommend that any employee considering purchasing a RAD to connect with the State's email system check first to confirm with the seller that the device will work with Microsoft ActiveSync, 2010.

- b. Due to the risks involved should any RAD become infected with viruses, the State has configured its ActiveSync interface to enable industry standard security settings. It's important to understand that once attached to the State's ActiveSync interface, a RAD will automatically have its security settings set to industry standard security settings. This may change the behavior of some settings; examples may include but are not limited to password length and time to lock out.
- c. At this time RAD devices such as iPads, iPhones, Droids, etc. are not able to be supported on the State's internal wireless network. However, BIT is actively seeking a cost effective way to allow such RADs to access the state's internal wireless network. Those staff authorized by their agency to use personally or state owned RAD devices will be notified if/when the State's internal wireless network would be available for use on their RAD.

### **3. Employee Use Agreement**

- a. While the State will make reasonable efforts to assure no personally owned data stored on or in a RAD device is lost or destroyed it is impossible to predict all circumstances that may arise. It's important, therefore, that anyone accessing State resources through a personally owned RAD device assume responsibility for backing up their personal data.
- b. Although most e-discovery requests or other legally mandated searches can be fulfilled through the State servers, the RAD owner agrees to surrender the RAD device to the appropriate technical authorities if it is required under the request.
- c. Should a breach of security occur on the RAD it may need to be remotely wiped and returned to factory settings. If a remote wipe is not possible the RAD owner may be asked to temporarily surrender the RAD to the State in order for it to be wiped.
- d. Should the RAD owner terminate employment with the State the RAD owner may, at the discretion of his/her supervisor, be asked to demonstrate that all State owned data is removed from the RAD. BIT can assist you or your supervisor in confirming that all state data has been deleted from a personal or state-owned RAD. If you would like such assistance, please contact the BIT Help Desk at: 773-Help (773-4357). The BIT Help Desk can provide or arrange assistance for you.
- e. Most modern RAD devices can be maintained and repaired only by their manufacturer or the original seller who would be licensed to have and use the unique tools and parts needed. Any other parties attempting to perform repairs will generally void warranties and may be a violation of contract terms. BIT cannot, therefore, perform maintenance on personally owned RADs. BIT can provide basic startup instructions to RAD users by contacting the BIT Help Desk. If a personally owned RAD device is unable to access the State's ActiveSync interface after BIT has confirmed that

interface is working correctly, the company who supports the device or their Help Desk should be contacted.

- f. To use the RAD for State email, special features, applications or data plans may be required which could add to the cost of the RAD service. The agency may decide to reimburse the RAD owner for all or partial cost of the RAD service.
- g. The State will not be liable for any damages caused by inappropriate use of the RAD. Inappropriate use could include damage to data done by someone hacking into the RAD, damage to data done by someone not authorized to use the RAD and sending inappropriate email or texts from the RAD.
- h. For legal and regulatory reasons, it's important that anyone accessing State email through a personal RAD device understand that all activities over the State email system while conducting State business remains the property of the State of South Dakota. Each agency may wish to review their own regulatory and data security needs to determine if further restrictions will be required for their own staff. Employees should be thoughtful when using personal RAD devices with multiple email accounts on them to assure they do not accidentally mix state business and personal business by responding to state business on personal email accounts or vice versa.

**4. Additional Concerns** – There are some other areas that agency decision makers will generally find of value. These points are gleaned from research of technology available today and from experience and recommendations of legal and business professionals.

- a. While the State acts to safeguard data, it is not possible to predict all possible situations or all possible technology interactions. It should be assumed, therefore, that any data on a RAD, either personal or State owned, is at risk of being lost or destroyed.
  - i. While it's true that the risk of theft of data is always present with portable devices, agency decision makers may want to consider whether the likelihood of theft should be a factor when deciding whether to authorize staff to download and store their data on personal devices.
- b. RAD security features differ based on manufacturer and operating system type. The State does not have access to manufacturers' internal security features for RAD's and not all types of RAD's are capable of downloading all industry standard security policies. As such, the level of security on RAD's will vary.
- c. Ediscovery laws have changed the definition of what constitutes a public record. Use of a RAD to send or receive email could result in the creation of public records which are discoverable under a court order. Any data on the RAD, personal or State owned could be made public.

- 5. Minimum Security Standards** - The RAD owner agrees to abide by the following minimum security standards if they are supported by the RAD.
  - a. Inactivity timer set at 15 minutes.
  - b. Lockout after 10 failed password attempts.
  - c. Use of a password of at least 8 characters with 1 number and 1 special character.
  - d. A RAD should not be shared with anyone not authorized to access the owners' State email account.
  
- 6. Loss or Theft of the RAD** - In the event of loss or theft of a RAD the owner must:
  - a. Notify the BIT Help Desk immediately
  - b. Change his/her Active Directory password

Notify the cellular company providing service to the RAD to have it wiped and/or deactivated.