Security Target Release 1.0 for Good Work System

EAL4
Augmented with
ALC_FLR.1

Good Technology Corporation
430 North Mary Avenue, Suite 200
Sunnyvale, CA 94085
1-866-7BE-GOOD
www.good.com

TABLE OF CONTENTS

DOCUMENT CONTROL

Document Owners			
Role	**Person**	**Telephone**	**Email**
Principal Security Product Manager	Rick Pitz	+1 408 212 7878	rpitz@good.com
Office of the CTO	Henry Hernandez	+1 408 212 7837	hhernandez@good.com

ABBREVIATIONS

Abbreviation	Description
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command-line interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
DES	Data Encryption Standard
DNS	Domain Name System
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GAL	Global Address List
GC	The Good Control Server
GEMS	The Good Enterprise Mobility Server
GP	The Good Proxy Server
GSC	Good Secure Cloud
IP	Internet Protocol
IT	Information Technology
OS	Operating System
OTA	Over-The-Air
RBA	Role-Based-Administration
SF	Security Function
SFP	Security Function Policy
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

1. Introduction (ASE_INT)

Identification

ST Title: Security Target Release 1.0 for Good Work System
CC Version: 3.1 Revision 4
Assurance level: EAL4 augmented with ALC_FLR.1
PP Identification: None
TOE name: Good Work System
TOE Version:

- Good Work System
- Product versions as described in Table 1

TOE Overview

Security Architecture

The Good Work System is an end to end solution for securing and managing email, calendar, contact, presence, instant messaging, secure browsing and other mobile applications. The Good Work System consists of server side and client side components. The server components include the Good Proxy Server, the Good Enterprise Mobility Server (GEMS), and the Good Control Server (administrative console functions). All servers run on standard Microsoft server platforms. On the client side, the Good Work System includes the Good Collaboration application, Good Access (secure browser) application, and other mobile applications running on iOS and Android devices using the Good Dynamics framework.

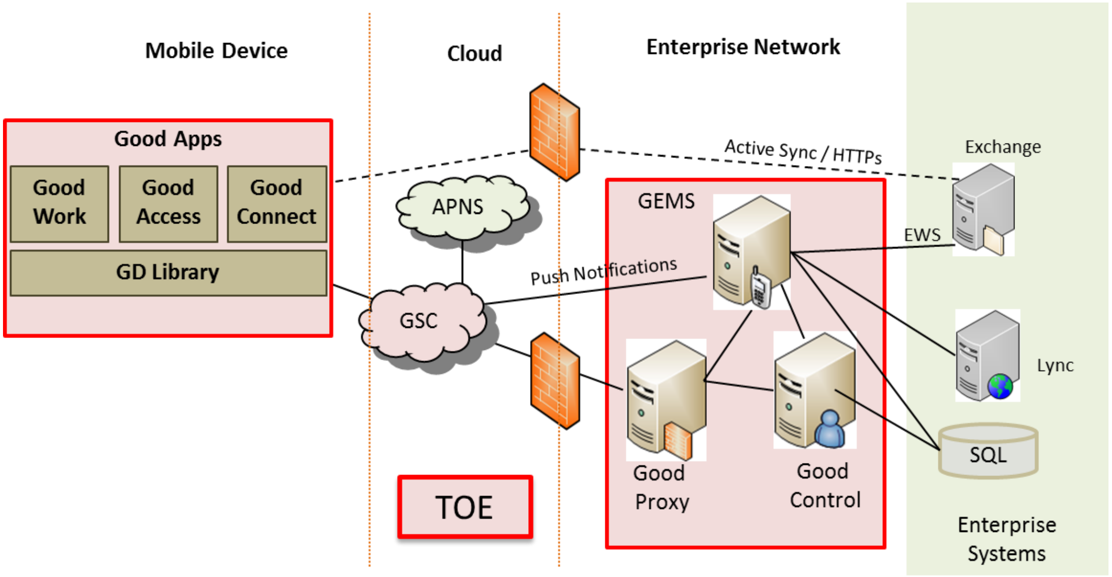

Figure 1; Core architecture

Good Control:
Good Control Server provides dashboard visibility and management of enterprise users, apps, and security policies.

Good Proxy:
Good Proxy Server provides the secure communications infrastructure between the Good Secure Cloud (GSC) and application servers within the enterprise firewall.

GEMS:
GEMS provides the following functionality for Good client applications:
The implementation of device facing Good Dynamics Server Side Services invoked by Good client applications using the Good Dynamics Services Framework. This includes a Service to provide Presence information for Contacts, a Service to provide storage and synchronization of application data, and delivery of Push Notifications via the GSC, in response to updates detected for user mailboxes.

Good Work Client:
Good Work Client is a mobile device application that provides for secure email, calendar, contacts, presence and other mobile applications. Email is delivered to the client using Microsoft Exchange Active Sync.

Good Access Client:
Good Access Client is a secure web browser application for accessing corporate web-based resources from a remote device.

Good Connect Client:
Good Connect Client is an instant messaging application that integrates with the enterprise desktop Microsoft Lync system.

Good Dynamics Library:
Good Dynamics Library is a client SDK implementing a set of APIs used to configure and enforce user authentication, secure communications, and secure storage on both sides of the enterprise firewall. The Good Dynamic Client provides several functions to secure Good Applications on the mobile device, including application encryption and policy controls, encrypting data in motion, providing application level authentication, providing secure inter-application communications, enables policy controls and ability to change policies dynamically.

Hardware/Software/Firmware requirements

TOE hardware/software/firmware requirements are specified in Table 1: Platforms for TOE. TOE Environment (non-TOE) hardware/software/firmware requirements are specified in Table 1: Platforms for TOE Environment.

Product Identification

Product or Service Name:	Good Work System
Version:	1.0
Platforms (for Products):	Identified in Table 1. Note that all platforms are 64-bit versions.

Operating System / Product	Version	Component	Version
Platforms for TOE Environment			
Microsoft Windows Server	2008 2012	Microsoft SQL Server	2008 2012
		Oracle XE SQL Server	10g 11g

Microsoft Windows Server	2008 2012	Microsoft Lync Server	2010 2013
Microsoft Windows Server	2008 2012	Microsoft Exchange Server	2010 2013
Platforms for TOE			
Microsoft Windows Server	2008 2012	Good Proxy Server	2.0.3.7
Microsoft Windows Server	2008 2012	Good Enterprise Mobility Server	1.5.35.45
Microsoft Windows Server	2008 2012	Good Control Server	2.0.3.11
Apple iPhone & iPad iOS Device	9.x 8.x	Good Work Client Good Access Client Good Connect Client Good Dynamics SDK	1.5.3.247 2.4.3.734 2.3.10.0.458445.12 2.0.4413
Google Android Device	4.x 5.x	Good Work Client Good Access Client Good Connect Client Good Dynamics SDK	1.5.3.162 2.4.3.657 2.3.10.0.456604.571 2.0.1226

Table 1; Platforms

User/Administrator Documentation

The following is a list of the user and administrator guidance documents:

- Good Access Secure Browser Product Guide
- Good Access Secure Browser Release Notes
- Good Control / Good Proxy Server Installation Guide
- Good Proxy Server Release Notes
- Good Control Server Release Notes
- Kerberos Constrained Delegation for Good Dynamics
- Good Dynamics Server Scalability and Deployment Planning Guide
- Good Dynamics Secure Mobile Platform – An Overview for Administrators and Developers
- Good Dynamics Direct Connect Feature Summary and Configuration Guide
- GEMS Administrators Guide
- GEMS Release Notes
- Good Work Product Guide
- Good Work Release Notes
- Good Connect User Guide
- Good Connect Release Notes

TOE Description

The Good Work System provides Android and iPhone mobile users with a wirelessly synchronized connection to their company servers, so they can access up-to-date corporate email, attachments, contacts, calendar, public folders, global address lists, Presence, Instant Messaging, Secure Browsing and other mobile application data when away from their desks. The Good Work System is a complete, secure wireless system for accessing corporate messaging and data from behind the firewall on the mobile device.

The Good Work system includes:

- The Good Work Client, running on iOS and Android mobile devices (phones and tablets), providing secure email, calendar, contacts, presence, and other mobile applications.

- The Good Access Client, running on iOS and Android mobile devices (phones and tablets), providing secure browser functionality.
- The Good Connect Client, running on iOS and Android mobile devices (phones and tablets), providing secure instant messaging functionality.
- The Good Dynamics framework for securing mobile applications on iOS and Android devices (phones and tablets)
- The Good Proxy server running on a standard Microsoft server platform, providing secure communications between the enterprise servers running behind the firewall and the GSC.
- The Good Control server running on a standard Microsoft server platform, providing dashboard visibility and management of enterprise users, apps, and security policies.
- The Good Enterprise Mobility Server running on a standard Microsoft server platform, implementing various application services such as Presence information for Contacts, a Service to provide storage and synchronization of application data, and delivery of Push Notifications via the GSC, in response to updates detected for user mailboxes.

Wireless Synchronization

Good for Enterprise provides automatic synchronization of email, calendar, and contacts, between the user's Microsoft Exchange Server account and iPhone and Android mobile devices.

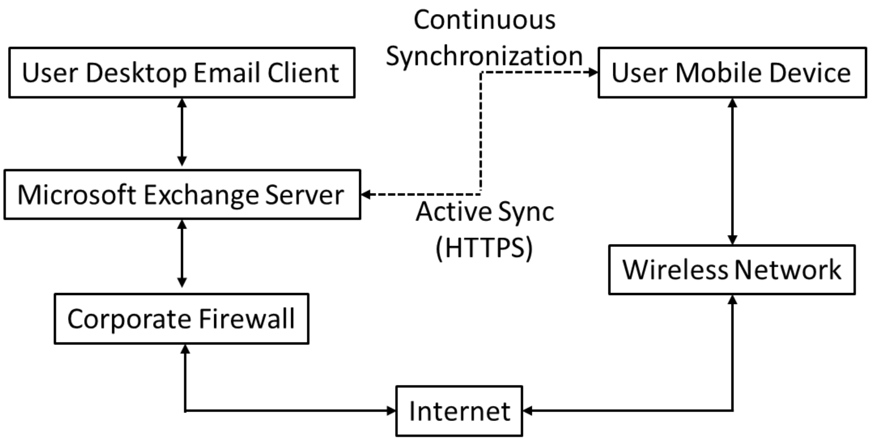

Figure 2; Synchronizing Exchange account and mobile device

As shown in Figure 2, Microsoft Active Sync is used to synchronize the users mobile device data with their desktop messaging system. The connection between the Active Sync server and the user's mobile device is secured with an HTTPS connection.

Good Work System Security Architecture

The Good Work System provides an end-to-end system designed to protect corporate information at all times—while it is being transmitted over the wireless network and while it resides on the mobile device. Installation of Good applications does not require any modifications to the customer's firewall, and allows leveraging the existing network security infrastructure.

Network Perimeter Security

Connections from the GEMS to the Good Secure Cloud (GSC) use HTTP and are protected by the Secure Sockets Layer (SSL). Connections to the GSC are used for authentication and for sending data to and receiving data from mobile devices. Perimeter security includes:

- End-to-end encryption
- AES-256
- Reliable message delivery

Mobile Device Security

The mobile device can be configured with a device password[1]. The Good application has its own password that is independent of the device password. When the mobile device is locked, Good applications will not display any of the user's data. Access to the Good Application can be restored only by entering the correct Good password. If an unauthorized user tries to guess the password too many times, the Good client software can be configured to lock the device or delete all Good application data stored on it.

The IT administrator can specify policies for the password provided by the user. These policies are applied wirelessly. Good data is encrypted and cannot be downloaded from the device.

If a user's mobile device is lost or stolen, the IT administrator can use the Good Control Console to remotely disable access to Good on the device and remove all Good application data.

When a user tries to access a corporate resource using the Good Work Application, the user would typically be prompted for their username and password (e.g. Active Directory credentials) in order to access that service. Alternately, the user can use Kerberos Constrained Delegation (KCD) in lieu of username and password. This allows the user to access network resources without exposing their credentials. KCD uses tickets that are encrypted and decrypted using secret keys that are not related to the user's credentials.

The client application utilizes the OpenSSL FIPS validated crypto library for all crypto functions related to data at rest protection (secure container data storage) and data in transit protection (data exchanged with Good servers).

Mobile Device Authentication

The Good Work System provides a number of safeguards against unauthorized access. The GEMS reside behind a corporate firewall, and any mobile device attempting to contact the servers require a three-step authentication process:

- the GSC and the GEMS
- the Good Work app on the mobile device and the GSC
- the Good Work app on the mobile device and the GEMS

Administrative Security

The Good Work System offers Role-Based-Administration (RBA) features that allow system-administration permissions to be customized according to the needs and qualifications of each user. By controlling users' access according to their roles and the associated permissions, RBA provides a tool for managing IT assets and increasing security.

[1] Password is not mandatory, but is always recommended by Good. The enterprise can choose to not have device passwords based on enterprise policy.

Good Secure OTA Architecture

OTA Deployment Security Considerations

In order to protect all traffic between Good OTA Setup and the Good servers, all communication during the provisioning process runs over HTTP/SSL. The package of provisioning information is further encrypted using an AES key derived from the user's OTA PIN. After the client receives the package of provisioning information, it begins to use the normal end-to-end encryption capabilities based on the server or application in use.

OTA Software Installation Security Considerations

The Good OTA software distribution system supports distribution of three classes of software: Good applications, Good partner applications, and custom applications provided by a customer's internal IT department. Security is maintained via the following:

- Digital Signatures - Good software and partner software are digitally signed using X.509v3 certificates.
- Encryption - Before the custom software package is uploaded, it is encrypted using a key generated by the GEMS.
- Software Versions - The Console provides a policy for IT to specify the minimum version of client software which will be installed.
- Mandatory Installation - IT can mark software packages as mandatory or optional.

Good Security Policies

Good Control allows the administrator to set a wide variety of policies to be enforced on user mobile devices. These include passwords; mandatory or permitted applications, databases, and folders; S/MIME; and other policies.

Managing User Accounts

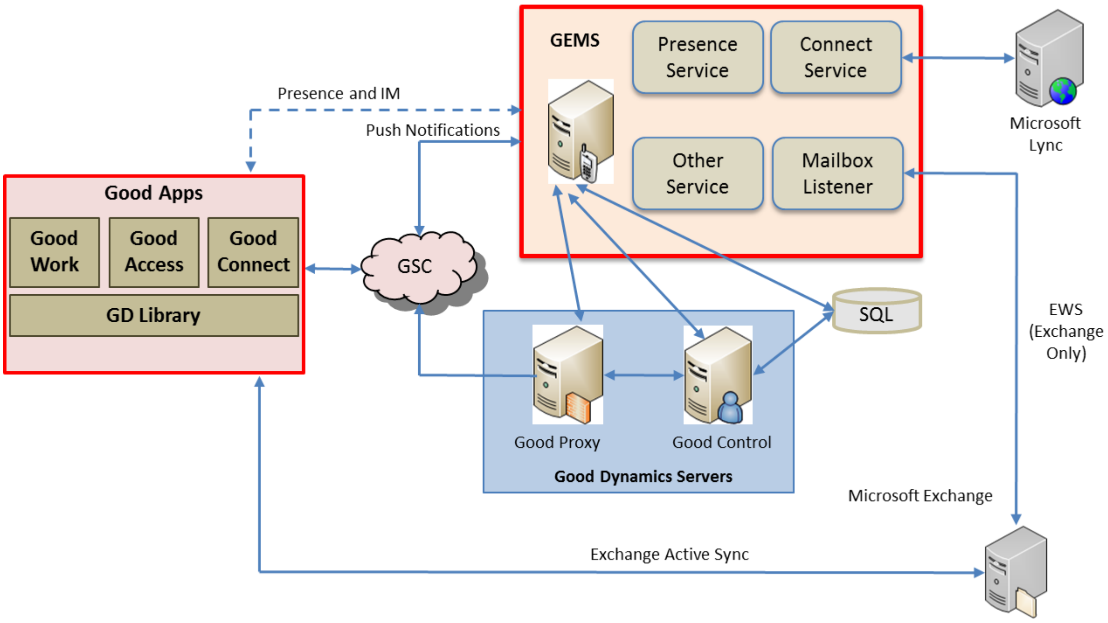

Figure 3; Managing the User Accounts

As shown in Figure 3, the GEMS provides presence information to the user's client on the mobile device. Active Sync (from Microsoft Exchange servers) is used to provide synchronization of email, calendars, etc. However, due to inactivity and other events, the client application may be terminated, but the user may still want to be notified when new mail is available. The GEMS monitors the exchange server via an Exchange Web Services (EWS) connection to the Exchange Server and uses Push Notifications to ensure that the client application has current information for things like email and calendar events. The Good Control server is used to manage policies that are pushed to the clients.

Managing roles

The role Superuser is granted all rights and can perform some tasks that no other user can perform. The Superuser must run the Good Control Console the first time it is accessed, and can then grant access to other accounts (using the Role Based Administration feature).

Roles such as service administrator, administrator, self-service and helpdesk can be defined in the Console, which then can be used to create, delete and reassign other roles when needed. The service administrator role is granted all rights in the TOE. The self-service role allows TOE users to optionally manage certain aspects of their mobile devices.

The Good Control Console is used to manage the mobile devices and servers, and to control and limit the tasks performed by an individual or group using Good Control Console. The console can be configured so that some individuals and groups can use it only to set up mobile devices and not to add or remove users, for example.

Data Encryption

All Good application data and folders on the mobile device are encrypted. This data is encrypted when Good Client applications are not using the data. The databases are decrypted as needed by the Good client applications.

Diagnostic Log File

Log files are maintained in clients and servers, and can be used by service personnel for troubleshooting purposes. Log files are encrypted and do not contain sensitive or personally identifiable information (PII). Sensitive information is obfuscated or removed prior to log files being written.

Corporate information

The TOE separates the mobile data into corporate and personal data, where only the corporate data are protected. Corporate authentication is not required to access personal data, since the personal data is not protected.

The rest of this document is only targeting protected corporate information.

Excluded Functions

The following product features have been excluded from the CC evaluated configuration:

- Windows clients are not part of this evaluation
- Domino server interface to GEMS is not supported in this evaluation
- Cloud service is not part of this evaluation
- GFE Client is not part of this evaluation (GFE is covered under separate evaluation).

Notations and Formatting

The notations and formatting used in this ST are consistent with Version 3.1 Revision 4 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text in square brackets, [*Selection value*].

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value with bold face in square brackets, **[Assignment_value]**.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration letter following the component identifier.

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threat agents are given names beginning with "TA." – e.g., TA.User. Threats to the TOE are given names beginning with "TT." – e.g., TT.Filter_Fails. TOE security environment threats are given names beginning with "TE."-- e.g., TE.Crypto_Fails.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter-msg and OE.Clearance.

2. CC Conformance Claim (ASE_CCL)

This TOE and ST are conformant with the following specifications:

- CC Part 2: Security functional components, September 2012, Version 3.1, Revision 4, extended.
- CC Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, conformant,
- Package: EAL4
- Protection Profiles: None
- Augmented SARs: ALC_FLR.1

3. Security Problem Definition (ASE_SPD)

Threats to security

Assets

AS.Corporate_Information: Corporate information on GEMS and Good client applications running on mobile devices.

Threat Agents

TA.Malicious_Actor: Malicious actors trying to get intelligible information stored on mobile devices or from communications between mobile devices, between mobile devices and servers, and between servers.

TA.Unauthorized_user: Individuals who have not been granted the right to access the system.

Identification of Threats

Threats to the TOE

TT.Eavesdropping: Malicious actor(s) eavesdropping on intelligible information on mobile devices, and/or data communications in transit between mobile devices.

TT.Theft: A malicious actor or an unauthorized user may get access to corporate information on the mobile device, by theft and/or loss of mobile devices.

TT.Tampering: An unauthorized user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.

TT.Access_Info: A malicious actor passes off as a mobile device user, and erases the corporate information on the mobile device.

TT.Mod_Conf: A malicious actor or an unauthorized user may modify the TOE configuration to gain unauthorized access to mobile devices.

Organizational security Policies

P.Secure_Communications: The TOE shall use secure communications functions for its own use, including encryption/decryption operations.

P.Manage: The TOE shall only be managed by authorized administrators.

P.Restrict: Changes made by administrators to default values in policies shall be more restrictive.

Assumptions

A.Install: The TOE has been installed and configured according to the appropriate installation guides, and all traffic between clients and servers flows through it.

A.Manage: There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it contains.

A.No_Evil: The administrators of the TOE are non-hostile, appropriately trained, and follow all guidance.

A.Locate: The processing resources of the TOE servers will be located within controlled access facilities, which will prevent unauthorized physical access.

4. Security objectives (ASE_OBJ)

TOE Security Objectives

O.Secure_Communications: The TOE shall use secure communications functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted to the TOE.

O.Protect: The TOE must ensure the integrity of audit, system data and corporate information by protecting itself from unauthorized modifications and access to its functions and data, and preserve correct operations during specified failure events.

O.Admin: The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE administrators with the appropriate training and privileges and only those TOE administrators, may exercise such control.

O.Authenticate_Admin: The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.

O.Authenticate_User: The TOE must be able to identify and authenticate users prior to allowing access to Good applications and data.

O.Audit: The TOE must record the actions taken by administrators, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.

O.Access_Int: The TOE must allow access to server resources on protected/internal network only as defined by the Access Control SFP.

Operational Environment Security Objectives

OE.Secure_Communications: The Operational Environment will provide secure communications functions to the TOE including encryption and decryption functions.

OE.Manage: Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.

OE.Physical: The physical environment must be suitable for supporting TOE servers in a secure setting.

OE.Install: Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.

Security Objectives Rationale

This section gives the relation between security objectives and threats, policies, and assumption.

Objectives	Threats, Assumptions, Policies	TT.Eavesdropping	TT.Theft	TT.Tampering	TT.Access_Info	TT.Mod_Conf	P.Secure_Communications	P.Manage	P.Restrict	A.Install	A.Manage	A.No_Evil	A.Locate
O.Secure_Communications		x	x				x						
O.Protect		x		x	x	x		x					
O.Admin								x	x				
O.Authenticate_Admin						x		x					
O.Authenticate_User			x		x			x					
O.Audit			x	x	x	x							
O.Access_Int		x						x					
OE.Secure_Communications		x	x				x						
OE.Manage						x				x	x	x	
OE.Physical													x
OE.Install								x		x	x		
OE.Person								x			x	x	

Table 2; Tracing of objectives to threats, assumptions, and policies

Threats

TT.Eavesdropping

The threat **TT.Eavesdropping** is met by the objectives **O.Secure_Communications**, **O.Protect and O.Access_Int**. **O.Secure_Communications** ensures that secure communication functions can maintain the confidentiality and allow for detection of modification of user data that is transmitted to the TOE. **O.Protect** ensures that the protection mechanisms of the TOE designed to prevent tampering with TOE IT assets are in place and functioning properly, and that these mechanisms cannot be bypassed. **O.Access_Int** ensures that access to server resources on protected/internal network is allowed only as defined by the Information Flow Control SFP. **OE. Secure_Communications** ensures that the secure communications functions include encryption and decryption.

TT.Theft

The threat **TT.Theft** is met by the objectives **O.Secure_Communications**, **O.Authenticate_User** and **O.Audit**. **O.Secure_Communications** ensures that secure communication functions can maintain the confidentiality and allow for detection of modification of user data that is transmitted to the TOE. **O.Authenticate_User** ensures that users identify and authenticate themselves before they are given access. **O.Audit** ensures that events of security relevance are audited. **OE. Secure_Communications** ensures that the functions include encryption and decryption.

TT.Tampering

The threat **TT.Tampering** is met by the objectives **O.Protect and O.Audit**. **O.Protect** ensures that the protection mechanisms of the TOE designed to prevent tampering with

TOE IT assets are in place and functioning properly, and that these mechanisms cannot be bypassed. **O.Audit** ensures that changes to the TOE will be recorded.

TT.Access_Info

The threat **TT.Access_Info** is met by the objectives **O.Protect**, **O.Authenticate_User and O.Audit**. **O.Protect** ensures that the TOE protects corporate information from unauthorized modifications. **O.Authenticate_User** ensures that users identify and authenticate themselves before they are given access. **O.Audit** ensures that events of security relevance are audited.

TT.Mod_Conf

The threat **TT.Mod_Conf** is met by the objectives **O.Protect**, **O.Authenticate_Admin**, **O.Audit** and **OE.Manage. O.Protect** ensures that the TOE protects configuration data from unauthorized modifications. **O.Authenticate_Admin** ensures that Administrators identify and authenticate themselves before they are given access to configuration data. **O.Audit** ensures that events of security relevance are audited. **OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user’s configuration data.

Policies

P.Secure_Communications

The policy **P.Secure_Communications** is met by the objective **O.Secure_Communications** and the Operational Environment Objective **OE. Secure_Communications** which will require the TOE to use secure communications services provided by the Operations Environment. These services will provide confidentiality and integrity protection of TSF data while in transit to the TOE.

P.Manage

The policy **P.Manage** is met by the objectives **O.Protect**, **O.Admin**, **O.Authenticate_User O.Authenticate_Admin**, **O.Access_Int, OE.Install** and **OE.Person**. The **O.Protect** objective provides for TOE self-protection. The **O.Admin** objective ensures there is a set of functions for administrators to use. The **O.Authenticate_User** objective provides for authentication of users prior to any TOE function accesses. The **O.Authenticate_Admin** objective provides for authentication of administrators prior to any management functions in the TOE. The **OE.Install** objective supports the **OE.Person** objective by ensuring administrator follow all provided documentation and maintain the security policy. The **O.Access_Int** ensures that the TOE limits access to internal network resources to the authorized users.

P.Restrict

The policy **P.Restrict** is met by the objective **O.Admin** by ensuring that the TOE provides a set of functions that allow management of its functions and data.

Assumptions

A.Install

The assumption **A.Install** is met by the objectives **OE.Manage** and **OE.Install. OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user’s configuration data. **OE.Install** ensures that the TOE will be installed correctly and configured securely. All traffic between the internal and external networks will flow through the TOE.

A.MANAGE

The assumption **A.Manage** is met by the objectives **OE.Manage, OE.Person** and **OE.Install. OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data and who will periodically check the accuracy of the TOE's timestamps. **OE.Person** objective will ensure that administrators follow all provided documentation and maintain the security policy. **OE.Install** ensures that the TOE will be installed correctly and configured securely.

A.NO_EVIL

The assumption **A.No_Evil** is met by the objectives **OE.Manage** and **OE.Person. OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data and who will periodically check the accuracy of the TOE's timestamps. **OE.Person** objective will ensure that administrators follow all provided documentation and maintain the security policy.

A.LOCATE

The assumption **A.Locate** is met by the objectives **OE.Physical**. **OE.Physical** ensures that the TOE's environment is suitable for securely supporting the TOE.

5. Extended Components Definition (ASE_ECD)

FDP_SWA_EXP.1 Secure Web Access

Management:
The following actions could be considered for the management functions in FMT:
Enabling the secure web access function on mobile devices.

Audit: There are no auditable events foreseen.

Hierarchical to: No other components.
Dependencies: None.

FDP_SWA_EXP.1.1 The TSF shall provide secure intranet web browsing access capabilities.

FPT_ITT_EXP.1 Basic internal TSF data transfer protection

Management: There are no management functions foreseen.

Audit: There are no auditable events foreseen.

Hierarchical to: No other components.
Dependencies: None.

FPT_ITT_EXP.1.1 The TSF shall use mechanisms from the Operational Environment to protect TSF data from [*selection: disclosure, modification*] when it is transmitted between separate parts of the TOE.

FTP_ITC_EXP.1 Inter-TSF trusted channel

Management: There are no management functions foreseen.

Audit: There are no auditable events foreseen.

Hierarchical to: No other components.
Dependencies: None

FTP_ITC_EXP.1.1 The TSF shall use a communication channel provided by the Operational Environment to communicate between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_EXP.1.2 The TSF shall permit [*selection: the TSF, another trusted IT product*] to communicate via the trusted channel.

FTP_ITC_EXP.1.3 The TSF shall communicate via the trusted channel for [**assignment: list of functions for which a trusted channel is required**].

FTP_TRP_EXP.1 Inter-TSF Trusted path

Management: There are no management functions foreseen.

Audit: There are no auditable events foreseen.

Hierarchical to: No other components.

Dependencies: None

FTP_TRP_EXP.1.1 The TSF shall use a communication path provided by the Operational Environment to communicate between itself and [*selection: remote, local]*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *[selection: modification, disclosure,* **[*assignment: other types of integrity or confidentiality violation*]**].

FTP_TRP_EXP.1.2 The TSF shall permit [*selection: the TSF, local users, remote users*] to communicate via the trusted path.

FTP_TRP_EXP.1.3 The TSF shall require the use of the trusted path for *[*selection: initial user authentication, **[assignment:** ***other services for which trusted path is required*]].**

FDP_CDD_EXP.1 Client data deletion

Management: There are no management functions foreseen.

Audit: Successful mobile device wipe action.

Hierarchical to: No other components.
Dependencies: None.

FDP_CDD_EXP.1.1 The TSF shall erase all enterprise user data stored within the mobile device when the following events occur: [**assignment: action taken**].

Extended Components Rationale

The extended components were created because the Common Criteria standard classes do not have any Security Functional Requirements (SFR) that accurately describe the unique capabilities of this TOE solution. The table below provides the rationale for each extended component used in this ST.

Explicit Component	Identifier	Rationale
FDP_SWA_EXP.1	SECURE WEB ACCESS	This explicit component is necessary since it describes product-unique functionality, consisting of secure web access from the Client.
FPT_ITT_EXP.1	BASIC INTERNAL TSF DATA TRANSFER PROTECTION	This explicit component is necessary since it provides the ability for the TOE to use secure communications capabilities provided by the Operational Environment.
FTP_ITC_EXP.1	INTER-TSF TRUSTED CHANNEL	This explicit component is necessary since it provides the ability for the TOE to use a trusted communication channel provided by the Operational Environment to communicate between itself and another trusted IT product.
FTP_TRP_EXP.1	INTER-TSF TRUSTED PATH	This explicit component is necessary since it provides the ability for the TOE to use a trusted communication channel provided by the Operational Environment to communicate between itself and users.

FDP_CDD_EXP.1	CLIENT DATA DELETION	This explicit component is necessary since it describes product-unique functionality to wipe mobile device enterprise data.

6. Security Requirements (ASE_REQ)

Security Functional Requirements (SFRs)

Functional Components	
Security Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.1B	Client audit data generation
FAU_GEN.2	User identity association
User Data Protection	
FDP_ACC.1A	Subset access control - Administrator
FDP_ACC.1B	Subset access control - User
FDP_ACF.1A	Security attribute based access control - Administrator
FDP_ACF.1B	Security attribute based access control - User
FDP_ITC.2	Import of user data with security attributes
FDP_SWA_EXP.1	Secure web access
FDP_CDD_EXP.1	Client Data Deletion
Identification and Authentication	
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1A	Timing of authentication - Administrator
FIA_UAU.1B	Timing of authentication - User
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
Security Management	
FMT_MOF.1A	Management of security functions behaviour - Administrator
FMT_MOF.1B	Management of security functions behaviour - User
FMT_MSA.1A	Management of Security Attributes - Administrator
FMT_MSA.1B	Management of Security Attributes - User
FMT_MSA.3A	Static Attribute Initialisation - Administrator

FMT_MSA.3B	Static Attribute Initialisation - User
FMT_SMF.1A	Specification of management functions - Administrator
FMT_SMF.1B	Specification of management functions - User
FMT_SMR.1	Security roles
Protection of the TSF	
FPT_ITT_EXP.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
Trusted Channel/Path	
FTP_ITC_EXP.1	Inter-TSF trusted channel
FTP_TRP_EXP.1	Inter-TSF trusted path

Security Audit (FAU)

FAU_GEN.1 Audit data generation

Dependences: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [**See Table 3 - Auditable Events**].

SFR	Auditable Event	Log Location
FAU_GEN.1	None	N/A
FAU_GEN.1B	None	N/A
FAU_GEN.2	None	N/A
FDP_ACC.1A	None	N/A
FDP_ACC.1B	None	N/A
FDP_ACF.1A	Successful requests to perform management functions	GC
FDP_ACF.1B	Successful requests to access corporate data (e.g., email)	Client
FDP_ITC.2	Successful import of user data from Exchange	Client
FDP_SWA_EXP.1	None	N/A
FDP_CDD_EXP.1	Successful mobile device wipe action.	GC
FIA_AFL.1	None	N/A
FIA_ATD.1	None	N/A
FIA_UAU.1A	Unsuccessful use of the authentication mechanism;	GC
FIA_UAU.1B	None	N/A
FIA_UID.1	None	N/A

FIA_USB.1	None	N/A
FMT_MOF.1A	All modifications in the behaviour of the console functions in the TSF.	GC
FMT_MOF.1B	All modifications in the behaviour of the console functions in the TSF.	GC
FMT_MSA.1A	All modifications of the values of security attributes.	GC
FMT_MSA.1B	All modifications of the values of security attributes.	GC
FMT_MSA.3A	None	N/A
FMT_MSA.3B	Modifications of the default setting of restrictive rules.	GC
FMT_SMF.1A	Use of managing administrator identifiers; creating, modifying, deleting role definitions.	GC
FMT_SMF.1B	Use of the console management functions.	GC
FMT_SMR.1	Modifications to the group of users that are part of a role;	GC
FPT_ITT_EXP.1	None	N/A
FPT_STM.1	None	N/A
FPT_TDC.1	Successful use of TSF data consistency mechanisms.	GEMS GC
FTP_ITC_EXP.1	None	N/A
FTP_TRP_EXP.1	None.	N/A

Table 3 - Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP[2]/ST, [**None**].

FAU_GEN.1b Audit data generation - Client

Dependences: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [**Diagnostic information**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP[3]/ST, [**None**].

[2] Good Work System is not compliant to any protection profile.

[3] Good Work System is not compliant to any protection profile.

FAU_GEN.2 User identity association

Dependences: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

User Data Protection (FDP)

FDP_ACC.1a Subset access control - Administrator

Dependences: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1a The TSF shall enforce the [**Administrator Access Control SFP**] on [subjects: **administrators**, objects: **management tasks**, operations: **access**].

FDP_ACC.1b Subset access control - User

Dependences: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1b The TSF shall enforce the [**User Access Control SFP**] on [subjects: **users**, objects: **corporate data**, operations: **access**].

FDP_ACF.1a Security attribute based access control – Administrator

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1a The TSF shall enforce the [**Administrator Access Control SFP**] to objects based on the following: [subjects: **administrators**, subject attributes: **administrator roles**, object: **management tasks**, object attributes: **none**].

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**role-based administration setup**].

FDP_ACF.1.3a The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4a The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1B Security attribute based access control – User

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1b The TSF shall enforce the [**User Access Control SFP**] to objects based on the following: [subjects: **users**, subject attributes: **mobile device policy**, object: **corporate data**, object attributes: **none**].

FDP_ACF.1.2b The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**mobile device policy**].

FDP_ACF.1.3b The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4b The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ITC.2 Import of user data with security attributes

Dependencies: FDP_ACC.1 Subset access control
FTP_ITC.1 Inter-TSF trusted channel
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the [**network perimeter security SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**no additional rules**].

FDP_SWA_EXP.1 Secure Web Access

Dependencies: None.

FDP_SWA_EXP.1.1 The TSF shall provide secure intranet web browsing access capabilities.

FDP_CDD_EXP.1 Client data deletion

Dependencies: None.

FDP_CDD_EXP.1.1 The TSF shall erase all enterprise user data stored within the mobile device when the following events occur: [**The wipe enterprise data command is received**].

Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within* **[*3 to 12*]**] unsuccessful authentication attempts occur related to **[the number of unsuccessful authentication attempts since the last successful authentication**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*surpassed*], the TSF shall [**lock out mobile device**].

FIA_ATD.1 User attribute definition

Dependences: None.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[administrator identifier, roles]**.

FIA_UAU.1a Timing of authentication - Administrator

Dependences: FIA_UID.1 Timing of identification

FIA_UAU.1.1a The TSF shall allow **[secure HTTPS and SSL connection establishment for the purpose of transferring and accessing corporate data, administrator identification]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2a The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1b Timing of authentication - User

Dependences: FIA_UID.1 Timing of identification

FIA_UAU.1.1b The TSF shall allow **[secure connection establishment for the purpose of transferring and accessing corporate data, user identification]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2b The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1 Timing of identification

Dependences: None.

FIA_UID.1.1 The TSF shall allow **[secure connection for the purpose of transferring and accessing corporate data]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Dependences: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[administrator identifier, roles]**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**user security attributes are bound upon successful login**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**user security attributes do not change until user logs in after changes are made**].

SECURITY MANAGEMENT (FMT)

FMT_MOF.1A MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR - ADMINISTRATOR

Dependences:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

FMT_MOF.1.1a The TSF shall restrict the ability to [*determine the behaviour of*] the functions **[**

- **managing administrator identifiers,**
- **managing roles]**

- to **[administrators]**.

FMT_MOF.1B MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR - USER

Dependences:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles

FMT_MOF.1.1b The TSF shall restrict the ability to [*determine the behaviour of*] the functions **[**

- **managing user identifiers**
- **managing user password characteristics,**
- **managing mobile device policies]**

to **[administrators]**.

FMT_MSA.1A MANAGEMENT OF SECURITY ATTRIBUTES - ADMINISTRATOR

Dependencies:	FDP_ACC.1 Subset access control FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1a The TSF shall enforce the [**Administrator Access Control SFP**] to restrict the ability to [*query, modify, delete,* **[*create*]**] the security attributes **[**
administrator identifier,
administrator roles]
to **[administrators]**.

FMT_MSA.1B MANAGEMENT OF SECURITY ATTRIBUTES - USER

Dependencies:	FDP_ACC.1 Subset access control FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1b The TSF shall enforce the [**User Access Control SFP**] to restrict the ability to [*query, modify, delete,* **[*create*]**] the security attributes **[**
user identifier,
user password characteristics
mobile device policies]
to **[administrators]**.

FMT_MSA.3a Static attribute initialisation - Administrator

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1a The TSF shall enforce the [**Administrator Access Control SFP**] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a The TSF shall allow the [**administrators**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3b Static attribute initialisation - User

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1b The TSF shall enforce the [**User Access Control SFP**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2b The TSF shall allow the [**administrators**] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1a Specification of Management Functions - Administrator

Dependencies: None.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[**

- **managing administrator identifiers,**
- **creating, modifying, deleting role definitions**].

FMT_SMF.1b Specification of Management Functions - User

Dependencies: None.

FMT_SMF.1.1b The TSF shall be capable of performing the following management functions: **[**

- **managing user identifiers,**
- **managing user password characteristics,**
- **managing mobile device policies].**

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **[administrator, user].**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Protection of the TSF (FPT)

FPT_ITT_EXP.1 Basic internal TSF data transfer protection

Dependencies: None.

FPT_ITT_EXP.1.1 The TSF shall use mechanisms from the Operational Environment to protect TSF data from [*disclosure*] when it is transmitted between separate parts of the TOE.

FPT_STM.1 Reliable time stamps

Dependencies: None.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TDC.1 Inter-TSF basic TSF data consistency

Dependencies: None

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**protected corporate information**] when shared between the TSF and another trusted IT product[4].

FPT_TDC.1.2 The TSF shall use [**the Good Enterprise Mobility Server**] when interpreting the TSF data from another trusted IT product.

Trusted Path / Channels (FTP)

FTP_ITC_EXP.1 Inter-TSF trusted channel

Dependencies: None

FTP_ITC_EXP.1.1 The TSF shall use a communication channel provided by the Operational Environment to communicate between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_EXP.1.2 The TSF shall permit [*the TSF or another trusted IT product*] to communicate via the trusted channel.

FTP_ITC_EXP.1.3 The TSF shall communicate via the trusted channel for [**sending data to and from another trusted IT product**].

FTP_TRP_EXP.1 Inter-TSF Trusted path

Dependencies: None

FTP_TRP_EXP.1.1 The TSF shall use a communication path provided by the Operational Environment to communicate between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *[modification or disclosure]*.

FTP_TRP_EXP.1.2 The TSF shall permit [*the TSF*] to communicate via the trusted path.

FTP_TRP_EXP.1.3 The TSF shall require the use of the trusted path for [***communication to mobile devices***].

[4] Trusted IT products are Exchange mail servers, Lync servers, SQL servers, and other enterprise application servers.

Security Assurance Requirements (SARs)

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.1, ALC_LCD.1, ALC_TAT.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.3

Table 4; Assurance requirements EAL4 augmented with ALC_FLR.1

Security Requirements Rationale

This section gives the relation between SFRs and security objectives.

TOE functional requirements	**Objectives for the TOE**	O.Secure_Communication	O.Protect	O.Admin	O.Authenticate_Admin	O.Authenticate_User	O.Audit	O.Access_Int
Security Audit (FAU)								
FAU_GEN.1 Audit data generation							X	
FAU_GEN.1B Audit data generation - Client							X	
FAU_GEN.2 User identity association							X	
User Data Protection (FDP)								
FDP_ACC.1A Subset access control-Administrator					X			X
FDP_ACC.1B Subset access control-User						X		X
FDP_ACF.1A Security attribute based access control-Administrator					X			X
FDP_ACF.1B Security attribute based access control-User						X		X
FDP_ITC.2, Import of user data with security attributes								X
FDP_SWA_EXP.1, Secure Web Access				X				
FDP_CDD_EXP.1, Client Data Deletion								X
Identification and Authentication (FIA)								
FIA_AFL.1, Authentication failure						X		X

TOE functional requirements	**Objectives for the TOE**	O.Secure_Communication	O.Protect	O.Admin	O.Authenticate_Admin	O.Authenticate_User	O.Audit	O.Access_Int
handling								
FIA_ATD.1 User attribute definition					X	X		X
FIA_UAU.1A Timing of authentication-Administrator					X			X
FIA_UAU.1B Timing of authentication - User						X		X
FIA_UID.1 Timing of identification					X	X		X
FIA_USB.1 User-subject binding					X	X		X
Security Management (FMT)								
FMT_MOF.1A Management of security functions behaviour-Administrator				X				
FMT_MOF.1B Management of security functions behaviour-User				X				
FMT_MSA.1A Management of security attributes-Administrator				X				
FMT_MSA.1B Management of security attributes-User				X				
FMT_MSA.3A Static attribute initialisation-Administrator				X				
FMT_MSA.3B Static attribute initialisation-User				X				
FMT_SMF.1A Specification of Management Functions-Administrator				X				
FMT_SMF.1B Specification of Management Functions-User				X				
FMT_SMR.1 Security roles				X				
Protection of the TSF (FPT)								
FPT_ITT_EXP.1 Basic internal TSF data transfer protection		X	X					
FPT_STM.1 Reliable time stamps			X				X	
FPT_TDC.1, Inter-TSF basic TSF data consistency			X					
Trusted Path / Channels (FTP)								
FTP_ITC_EXP.1, Inter-TSF trusted channel		X	X					
FTP_TRP_EXP.1Inter-TSF Trusted path		X	X					

Table 5; Tracing of functional requirements to objectives

O.SECURE_COMMUNICATIONS

The TOE shall use secure communications provided by the Operational Environment to protect TSF data from disclosure when transmitted between separate parts of the TOE to meet **FPT_ITT_EXP.1**. The TSF shall use a communication channel provided by the Operational Environment to communicate between itself and another trusted IT product to meet the requirements of **FTP_ITC_EXP.1**. The TOE shall use a secure communications path between the Server and mobile device provided by the Operational Environment to satisfy **FTP_TRP_EXP.1**.

O.PROTECT

The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data. **FPT_ITT_EXP.1** requires the TOE to protect the collected data from disclosure when the data is transmitted to a separate part of the TOE. **FPT_STM.1** requires that the TOE provide reliable timestamps for its own use. **FPT_TDC.1** requires that the TSF shall provide the capability to consistently interpret all information when shared between the TSF and the enterprise mail server. **FTP_ITC_EXP.1** requires that the TSF shall provide a communication channel between itself and mobile devices that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. The TOE shall use a secure communications path between the TOE and administrators provided by the Operational Environment to satisfy **FTP_TRP_EXP.1.**

O.ADMIN

The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. **FMT_MOF.1A&B** restricts access to TOE management functions. **FMT_MSA.1A&B** specifies which roles can access security attributes. **FMT_MSA.3A&B** enforces the User Access Control SFP and Administrator Access Control SFP to provide default values for security attributes that are used to enforce the SFP and who can modify the default values. **FMT_SMF.1A&B** specifies the management functions the TOE must provide. **FMT_SMR.1** requires the TOE to maintain separate Administrator roles.

O.AUTHENTICATE_ADMIN

The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data**. FDP_ACC.1A** requires the TOE to enforce the Administrator Access Control SFP. **FDP_ACF.1A** specifies the attributes used to enforce the Administrator Access Control SFP. **FIA_ATD.1.1** defines security attributes of subjects used to enforce the authentication policy of the TOE. **FIA_UAU.1A** requires Administrators to be authenticated before they are able to perform any other actions. **FIA_UID.1** requires Administrators to be identified before they are able to perform any other actions. **FIA_USB.1** ensures that user security attributes are associated with subjects acting on the behalf of that user.

O.AUTHENTICATE_USER

The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data**. FDP_ACC.1B** requires the TOE to enforce the User Access Control SFP. **FDP_ACF.1B** specifies the attributes used to enforce the User Access Control SFP. **FIA_AFL.1** ensures that user data is not accessible when the defined number of unsuccessful authentication attempts has been met or surpassed. **FIA_ATD.1** defines security attributes of subjects used to enforce the authentication policy of the TOE. **FIA_UAU.1B** requires users to be authenticated before they are able to perform any other actions. **FIA_UID.1** requires users to be identified before they are able to perform any other actions. **FIA_USB.1** ensures that user security attributes are associated with subjects acting on the behalf of that user.

O.AUDIT

The TOE must record the actions taken by administrators and users, and provide reliable timestamps for its own use. **FAU_GEN.1** requires that the TOE records relevant commands entered by an Administrator. **FAU_GEN.2** requires that the TOE associates events with users. **FPT_STM.1** requires that the TOE provide reliable timestamps for its own use. **FAU_GEN.1B** ensures that diagnostic data is collected on the mobile device.

O.ACCESS_INT

The TOE must be able to identify and authenticate users and administrators prior to allowing access to TOE functions and data. **FDP_ACC.1A&B** requires the TOE to enforce the Administrator and User Access Control SFP. **FDP_ACF.1A&B** specifies the attributes used to enforce the Administrator and User Access Control SFP. **FIA_AFL.1** ensures that user data is not accessible when the defined number of unsuccessful authentication attempts has been met or surpassed. **FIA_ATD.1** defines security attributes of subjects used to enforce the authentication policy of the TOE. **FIA_UAU.1A&B** requires users and administrators to be authenticated before they are able to perform any other actions. **FIA_UID.1** requires users and administrators to be identified before they are able to perform any other actions. **FIA_USB.1** ensures that user and administrators security attributes are associated with subjects acting on the behalf of that user. **FDP_CDD_EXP.1** ensures that user data on the mobile device is erased when the administrator issues the remote wipe command. **FDP_ITC.2** requires the TOE to enforce the network perimeter security SFP when importing user data.

SFR DEPENDENCIES

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them.

Security functional requirement	Dependency	Rationale
	Security Audit (FAU)	
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included.
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	Included
	User Data Protection (FDP)	
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Included

Security functional requirement	Dependency	Rationale
FDP_ITC.2, Import of user data with security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	Included (FDP_ACC.1, FTP_TRP_EXP.1, FTP_TDC.1 and FTP_ITC_EXP.1,)
FDP_SWA_EXT.1 Secure Web Access	None	
FDP_CDD_EXP.1 Client Data Deletion	None	
Identification and Authentication (FIA)		
FIA_AFL.1, Authentication failure handling	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
Security Management (FMT)		
FMT_MOF.1 Management of security functions behaviour	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	Included
FMT_MSA.1 Management of security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included (FDP_ACC.1, FMT_SMR.1, FMT_SMF.1)
FMT_MSA.3 Static attribute initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_SMF.1 Specification of Management Functions	None	
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	Included
Protection of the TSF (FPT)		
FPT_ITT_EXP.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	

Security functional requirement	Dependency	Rationale
FPT_TDC.1, Inter-TSF basic TSF data consistency	None	
Trusted Path / Channels (FTP)		
FTP_ITC_EXP.1, Inter-TSF trusted channel	None	
FTP_TRP_EXP.1 Trusted path	None	

Table 6; Security functional requirements dependency rationale

SAR Rationale

This ST contains the assurance requirements from the CC EAL4 assurance package augmented with ALC_FLR.1. A major market for Good Technology is government agencies. A requirement from several of the government agencies is that we have this level (EAL4+) of Common Criteria certification.

7. TOE Summary Specification (ASE_TSS)

TOE Security Functions Specification

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 6.

List of security functions:

- Security_Audit
- Userdata_Protection
- Identification_Authentication
- Security_Management
- TSF_Protection
- Trusted_Path-Channels

SF.Security_Audit

The TOE provides a capability to generate and view events by recording them in a log file.

This GC Server log file records the administrative tasks performed by Good Control Console. It contains auditing information about when the tasks were performed and who performed them. Event messages are recorded in the Windows Event Viewer Application log. This log file records the server's/mobile device synchronization activity for messages and events. Synchronization error and event messages are recorded in the Windows Event Viewer Application log. Likewise, the GEMS and Good Proxy maintain log files for their respective operations.

The Client log file records diagnostic information. The Client log is stored in non-volatile memory and can be uploaded for diagnostic purposes.

SF_Userdata_Protection

The TOE supports access operation access with the subject attributes administrator roles and user roles. Administrator access to management tasks is restricted based on the assigned administrator role and the options within that role. User access to corporate data is restricted based on the assigned mobile device policy.

The TOE shall enforce network perimeter security when importing user data from outside of the TOE. Communications between the TOE and Domain Controllers and SQL Servers is protected by the Operational Environment.

Clients can be configured to use a secure web browser (Good Access) to access intranet web sites.

All administrators have to be authenticated. Good provides the capability of enforcing role based administration to separate administrative functions if so desired.

Administrators can wipe mobile device data with a remote wipe command from the Administrator's console.

SF.IDENTIFICATION_AUTHENTICATION

Administrator access of the Good servers is not a part of the domain. Therefore administrator access is being authenticated against Active Directory.

The Good Work System offers Role-Based-Administration (RBA) features that allow system-administration permissions to be customized according to the needs and qualifications of each user. By controlling users' access according to their roles and the associated permissions, RBA provides a tool for managing IT assets and increasing security.

The Good mobile client applications can be configured with a password. When the application is locked, Good applications will not display any of the user's data. Access can be restored only by entering the correct password. If an unauthorized user tries to guess the password exceeding the administrator-specified limit, the Good client software can be configured to lock the application or delete all Good application data stored on it.

SF.SECURITY_MANAGEMENT

Exchange Active Sync is used to synchronize the user's email, calendar, contacts, tasks, notes with their desktop application. For functions that are not supported via Active Sync, and to keep synchronization running when the application is not in the foreground, the GEMS has a process that listens for events from the Exchange server via an Exchange Web Services (EWS) interface. Such events are then pushed to the client using the Push Notification Service of the GEMS.

Good Control Server uses the Exchange Global Address List (GAL) to list, monitor, and manage mobile device users across sites. There must be at least one Good Control Server installed. To access the Console, administrators enter a URL to the Server. Console use is controlled by the roles that are assigned to the administrators who use it.

The Good Control Console is used to assign mobile devices to users and to monitor and manage other resources in the system. The Good Console manages the mobile devices and servers, and controls and limits the tasks performed by an individual or group using Good Control Console. The console can be configured so that some individuals and groups can use it only to set up mobile devices and not to add or remove users, by creating roles for different users and group of users for Good Control Console.

The Administrator role is created with access to all management functions. Administrators may change the default settings to restrict access to management functions. By default, the Administrator role has access to the following management functions:

- Mobile device rights
- Mobile device security rights
- Manage Mobile Service Settings
- Server rights
- Deployment Rights

Administrators create all user accounts with user identifiers and password characteristics. Mobile device user accounts are assigned mobile device policies created by the Administrator.

Administrators configure mobile device policies with the following restrictive default settings as shown in Table 7 – Mobile Device Policy Settings.

Mobile Device Policy Parameter	Setting
Client Password Related	

Password protected lock screen	N
Expire password after	60 days
Disallow previously used passwords	6
Minimum password length of	8 characters
Disallow repeated characters after	1 character
Require both letters and numbers	Y
Require both upper and lower case	Y
Require at least one special character	Y
Do not allow sequential numbers	Y
Lock Screen Protection	
Require password when idle for more than	15 minutes
Take action after __ invalid password attempts	3
Action to take	Wipe data
Show notifications on lock screen	N
Allow event reminder details over lock screen	N
Messaging	
Do not allow data to be copied from the Good application	Y
Do not allow data to be copied into the Good application	Y
Provisioning	
OTA Pin expires after	3 days
Allow OTA PIN reuse	N
iOS Specific Configuration	
Enable MDM profile	Y
Require passcode length of at least	8 char
Allow simple value	N
Alphanumeric	Y
Enable Remote Wipe	Y
Maximum failed attempts	3
Android Specific Configuration	
Enable full device remote wipe	Y
Enable remote full device lock	Y
Enable Remote Password reset	Y
Require passcode with minimum length of	8 char
Maximum failed passcode attempts	3
Good Access (Secure Browser)	
Enable access to the Intranet	Y

Table 7 – Mobile Device Policy Settings

Administrators can change the following mobile device policy default settings to be more restrictive:

- Enable password protected lock screen
- Expire password less than 60 days
- Disallow previously used passwords greater than 6
- Minimum password length greater than 8 characters
- Require password when idle for less than 15 minutes
- Take action after less than 3 invalid password attempts
- OTA PIN expires in less than 3 days
- Require iOS passcode length of greater than 8 characters
- Maximum iOS failed attempts less than 3
- Require Android passcode with minimum length of greater than 8 characters
- Maximum Android failed passcode attempts less than 3

SF.TSF_Protection

Specification of products is described in sections 1.2.2 and 1.2.3, where trusted IT products are Exchange Server, SQL Server, Lync Server. Data transmitted from the TSF to another trusted IT product is protected by the Operational Environment from unauthorized disclosure during transmission.

TSF data shall be protected when it is transmitted between separate parts of the TOE (e,g, GC to GEMS). The Operational environment will provide secured communication mechanisms used by the TOE data types that are transferred including e-mail, attachments, contacts, calendar, and browser.

The TOE provides timestamps for the TOE’s use in audit log timestamps.

Trusted_Path-Channels

The Good Work System provides an end-to-end system designed to protect corporate information at all times—while it is being transmitted over the wireless network and while it resides on the mobile device.

The information between GEMS and mobile devices is transferred via a secure communications mechanism provided by the Operational Environment and used by the TOE.

Connections from the GEMS to the GSC use HTTP and are protected by the SSL. Connections to the GSC are used only for sending data to and receiving data from mobile devices. Perimeter security includes:

- End-to-end encryption
- AES
- Reliable message delivery

Security Functions Rationale

The table below shows that all TOE security requirements can be traced to at least one TOE security function.

TOE functional requirements	Security audit	Userdata_Protection	Identification_Authentication	Security_Management	TSF_Protection	Trusted_Path-Channels
Security Audit (FAU)						
FAU_GEN.1 Audit data generation	X					
FAU_GEN.1B Audit data generation – Client	X					

TOE functional requirements	Security audit	Userdata_Protection	Identification_Authentication	Security_Management	TSF_Protection	Trusted_Path-Channels
FAU_GEN.2 User identity association	X					
User Data Protection (FDP)						
FDP_ACC.1A&B Subset access control		X				
FDP_ACF.1A&B Security attribute based access control		X				
FDP_ITC.2, Import of user data with security attributes		X				
FDP_SWA_EXP.1 Secure Web Access		X				
FDP_CDD_EXP.1 Client Data Deletion		X				
Identification and Authentication (FIA)						
FIA_AFL.1, Authentication failure handling			X			
FIA_ATD.1 User attribute definition			X			
FIA_UAU.1A&B Timing of authentication			X			
FIA_UID.1 Timing of identification			X			
FIA_USB.1 User-subject binding			X			
Security Management (FMT)						
FMT_MOF.1A&B Management of security functions behaviour				X		
FMT_MSA.1A&B Management of security attributes				X		
FMT_MSA.3A&B Static attribute initialisation				X		

TOE functional requirements	Security audit	Userdata_Protection	Identification_Authentication	Security_Management	TSF_Protection	Trusted_Path-Channels
FMT_SMF.1A&B Specification of Management Functions				X		
FMT_SMR.1 Security roles				X		
Protection of the TSF (FPT)						
FPT_ITT_EXP.1 Basic internal TSF data transfer protection					X	
FPT_STM.1 Reliable time stamps					X	
FPT_TDC.1, Inter-TSF basic TSF data consistency					X	
Trusted Path / Channels (FTP)						
FTP_ITC_EXP.1, Inter-TSF trusted channel						X
FTP_TRP_EXP.1 Trusted path						X

Table 8; Tracing of TOE functional requirements to TOE security functions

SF.Security_Audit

The TOE security function SF.Security_Audit, "The TOE provides a capability to generate and view events by recording them in a log file", meets the audit requirements **FAU_GEN.1** and **FAU_GEN.2.** Recording diagnostic information on the mobile devices is satisfied by **FAU_GEN.1B**.

SF.Userdata_Protection

The TOE security function SF.Userdata_Protection, "The TOE supports access operation access with the subject attributes administrator roles and user roles", meets the protection of user data requirements **FDP_ACC.1A, FDP_ACC.1B, FDP_ACF.1A, FDP_ACF.1B, FDP_ITC.2, FDP_SWA_EXT.1, and FDP_CDD_EXP.1.**

SF.Identification_Authentication

The TOE security function SF.Identification_Authentication, "The Good Work System offers Role-Based-Administration (RBA) features that allow system-administration permissions to be customized. When the mobile device is locked, Good applications will not display any of the user's data", meets the identification and authentication requirements **FIA_AFL.1, FIA_ATD.1, FIA_UAU.1A, FIA_UAU.1B, FIA_UID.1** and **FIA_USB.1.**

SF.Security_Management

The TOE security function SF.Security_Management, "The Good Control Console is used to assign mobile devices to users and to monitor and manage GEMS", meets the management requirements **FMT_MOF.1A, FMT_MOF.1B, FMT_MSA.1A, FMT_MSA.1B, FMT_MSA.3A, FMT_MSA.3B, FMT_SMF.1A. FMT_SMF.1B** and **FMT_SMR.1.**

SF.TSF_Protection

The TOE security function SF.TSF_Protection, "Data transmitted from the TSF to another trusted IT product is protected by the Operational Environment from unauthorized disclosure during transmission The TOE provides timestamps for the TOE's use", meets the protection of the TSF requirements **FPT_ITT_EXP.1, FPT_STM.1** and **FPT_TDC.1.**

SF.Trusted Path-Channels

The TOE security function SF.Trusted Path-Channels, the TOE uses secure communications channel mechanisms provided by the Operational Environment to exchange information with trusted external IT entities meets the Trusted Channel requirements **FTP_ITC_EXP.1.** The TOE uses secure communications path mechanisms provided by the Operational Environment to transfer data between the Server and Clients meets the trusted path requirement **FTP_TRP_EXP.1**.