NHS
Mansfield and Ashfield
Clinical Commissioning Group

NHS
Newark and Sherwood
Clinical Commissioning Group

Bring Your Own Device (BYOD) Policy

Document History

Document Reference:	
Document Purpose:	To set out the technical capabilities of the chosen security solution ‘Airwatch’ for the provision of corporate data to a personally owned device, via secure connection to a corporate ‘bubble’, within which corporate email can be viewed
Date Approved:	
Approving Committee:	Information Governance Management and Technology Committee
Version Number:	1
Status:	Approved
Next Revision Due:	January 2016
Developed by:	Information Governance, Greater East Midlands Commissioning Support Unit (GEM CSU)
Policy Sponsor:	Director of Outcomes and Information, South CCGs
Target Audience:	This policy applies to any person directly employed, contracted or volunteering with the CCG
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit

Revision History

Version	Date	Summary of Changes
0.1	November 2013	First draft for consultation
0.2	November 2014	Second Draft –NHIS capabilities statement for BYOD Mobile Device Management.

Policy Dissemination information

Reference Number	Title	Available from

To request connection of a Personally Owned device – please go to

https://customerportal.notts-his.nhs.uk/

And select the option equipment, and BYOD Connection.

Bring Your Own Device (BYOD) Policy

1 INTRODUCTION

This Policy applies to Nottinghamshire County Clinical Commissioning Groups CCGs), subsequently referred to in this document as the CCG(s). They include:

- NHS Mansfield and Ashfield CCG
- NHS Newark and Sherwood CCG
- NHS Nottingham North and East CCG
- NHS Nottingham West CCG
- NHS Rushcliffe CCG

The underlying feature of BYOD is that the user owns, maintains and supports the device. This means that the data controller will have significantly less control over the device than it would have over a traditional corporately owned and provided device.

Whilst ownership is not corporate, responsibility for the ownership of the data remains with the data controller, It is important to remember that the data controller must remain in control of the personal data for which he is responsible, regardless of the ownership of the device used to carry out the processing.

Connection of a personally owned device to corporate networks is subject to all organisational policy in respect of information security and the protection of data and equipment as listed at section 5.

2 PURPOSE

Bring Your Own device (BYOD) can be seen as a means of obtaining cost and resource efficiencies as the staff member may be providing the equipment e.g. Smartphone, Laptop etc. rather than the organisation purchasing this directly for them.

The purpose of this policy is to set out the technical capabilities of the chosen security solution 'Airwatch' for the provision of corporate data to a personally owned device, via secure connection to a corporate 'bubble', within which corporate email can be viewed.

Connections to clinical systems and or other data sources are achieved outside of Airwatch corporate bubble, for example for use to connect to clinical systems and data there are Mobile working solutions and VPN connectivity.
Mobile working solutions and VPN connections are only permitted on corporately owned devices, because of significant support requirements, device management and encryption, in addition to end user training requirements.

3 SCOPE

This policy applies to all employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff and volunteers) of the CCG. Third Parties with whom the CCG may agree information sharing protocols will be governed by this policy and associated information sharing agreements. Any user seeking to connect a personally owned device, must gain authority via their line management structures to connect and provide a budget code to meet the cost of the connection of the device to Airwatch, prior to the request being made to Nottinghamshire Health Informatics Service (NHIS) nhis.servicedesk@notts-his.nhs.uk.

4 DUTIES AND RESPONSIBILITIES

The CCG has a legal duty to comply with the Data Protection Act 1998. The Accountable Officer is responsible for ensuring that the responsibility for data protection is allocated appropriately within the CCG and that the role is supported.

All staff must adhere to CCG policies and procedures relating to the processing of personal information, and the Data controller must assure themselves that the technical solutions for the security of data are sufficient for the data being processed, specifically where these risks are increased through mobile working and personal ownership of devices. Specific policies of note for all BYOD users and authorisers are listed in section 5 below.

The capability assessment of Airwatch is contained at Appendix 2, as information for the product which is the supported solution provided via NHIS for the effective provision of Bring Your Own Device (BYOD).

5 ORGANISATIONAL POLICY

This policy should be read in conjunction with other relevant organisational Policies, including but not limited to:

- Information Security Policy
- Confidentiality and Data Protection Policy
- Email and Internet Policy
- Acceptable Use Policy
- Remote Working
- Information Risk

The CCGs grant their employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. The organisation reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined above.

This policy is intended to protect the security and integrity of the CCGs data and guard against both data leakage and data loss.

Employees remain subject to organisational policy and procedure in respect of personal conduct, data and information security, and physical security, including but not limited to those policies outlined above.

6 ACCEPTABLE USE

Employees remain subject to organisational policy and procedure in respect of personal conduct, data and information security, and physical security, including but not limited to those policies outlined above.

Of note for all organisational users in respect to mobile devices is that devices may not be used at any time to:

Store or transmit illicit material

Store or transmit proprietary information belonging to another organisation

Harass others

Engage in outside business activities

The CCG has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted – provided that it is safe and legal to do so.

7 DEVICES AND SUPPORT

NHIS Service Desk will discuss the connection of any device with the end user, to ensure that the device can be connected prior to organisational authorisation and purchase of Air watch licence and recurrent fee.

In regard to support, personal owned devices are not organisationally supported devices Only connectivity issues are supported by NHIS; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

If requested, devices must be presented to NHIS for 'proper job' provisioning and configuration of airwatch before they can access emails via the corporate bubble.

8 REIMBURSEMENT

The CCG will not reimburse the employee for the cost purchase or associated with the device: including but not limited to: Roaming charges, plan charges and overcharges, applications for personal use.

9 SECURITY

In order to prevent unauthorised access, devices are mandated to be password protected using the required 6 digit passcode, The CCG's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.

The device will lock itself with a password or PIN if it's idle for five minutes.

After ten failed login attempts, the device will sever the corporate connection to the network. Users must Contact NHIS to regain access.

Employees' access to the organisations data is limited based on user profiles defined by IT and automatically enforced.

The connection to the corporate bubble will be remotely wiped if:

1) the device is lost,

2) the employee terminates his or her employment,

3) IT detects a data or policy breach, a virus or similar threat to the security of the organisation's data and technology infrastructure.

For note for each organisation user and authoriser are associated risks of NHIS Service Desk Opening hours – Mon – Fri 08.00 to 18.00, excluding public holidays. Devices lost, stolen or otherwise compromised during times when the service desk is closed are to be reported as soon as possible following the event. Organisations instructing NHIS to undertake mobile device management services do so with an understanding and acceptance of this risk.

Provision of the corporate bubble includes a strong perimeter in that any content or attachments contained within the corporate bubble cannot be saved outside of the application or locally on the device, Any attempt to side step or circumvent security measures in place will be considered under the CCG disciplinary policies as outlined in policy requirements in section 5, for clarification this includes any attempt to 'screen capture' or otherwise photograph content to enable its onwards transmission outside of security parameters.

10 Risks/Liabilities/Disclaimers

The organisation reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices must be reported to the NHIS Service Desk within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the CCGs related acceptable use policies as referenced in section 5.

The employee is personally liable for all costs associated with his or her device.

The CCG reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy and those referenced as relevant in section 5.

13 Equality and Diversity

The CCG aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

14 Due Regard

This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

15 REFERENCES

Bring Your Own Device (BYOD) ..Information Commissioners Office
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

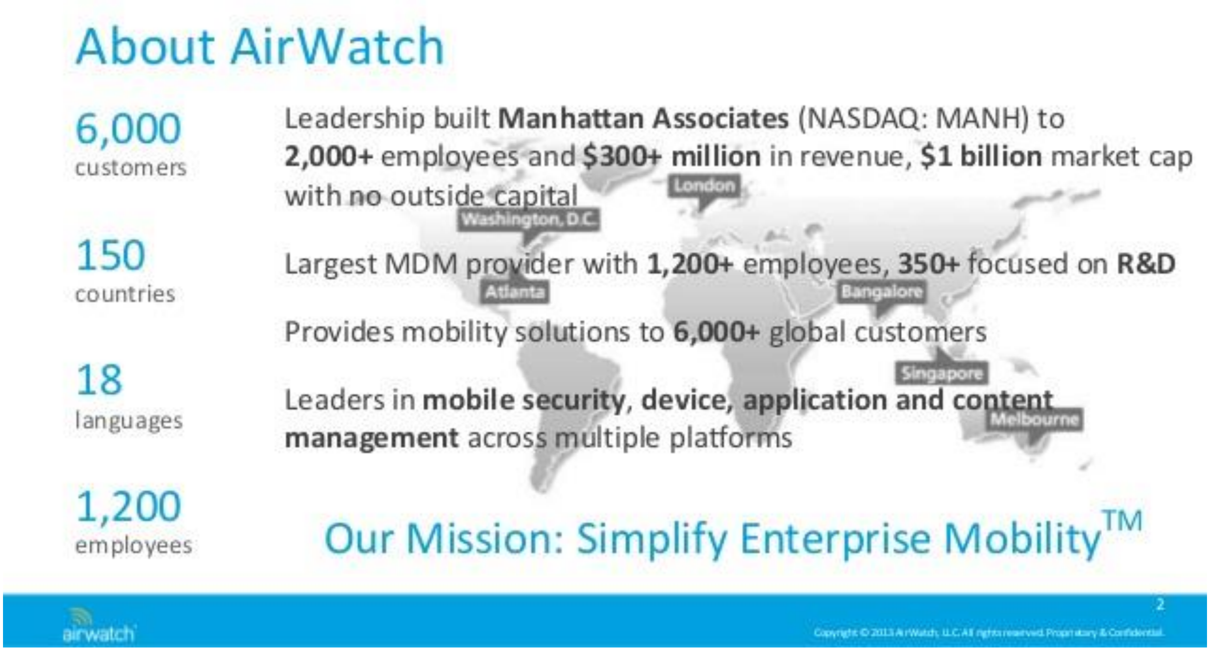
To request connection of a Personally Owned device – please go to

https://customerportal.notts-his.nhs.uk/

And select the option equipment, and BYOD Connection.

Appendix One: Airwatch Provision of Corporate Bubble and Security Arrangements:

NHIS chose Airwatch as Industry leader in the support and maintenance of secure mobile access solutions.



London
Washington, D.C.
Atlanta
Bangalore
Singapore
Melbourne

About AirWatch

6,000 customers

150 countries

18 languages

1,200 employees

Leadership built **Manhattan Associates** (NASDAQ: MANH) to **2,000+** employees and **$300+ million** in revenue, **$1 billion** market cap with no outside capital

Largest MDM provider with **1,200+** employees, **350+** focused on **R&D**

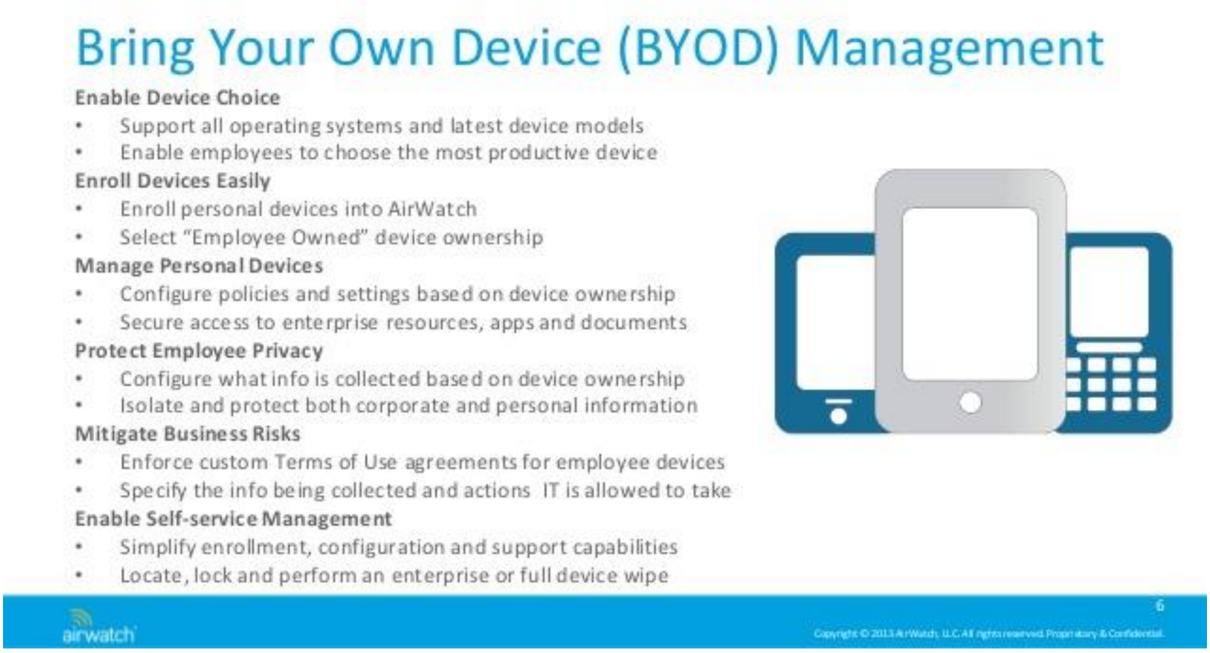
Provides mobility solutions to **6,000+** global customers

Leaders in **mobile security, device, application and content management** across multiple platforms

Our Mission: Simplify Enterprise Mobility™

2

In Support of BYOD, Airwatch has a wealth of features to enable the connection of personal devices within a controlled and assured connection provision.



Bring Your Own Device (BYOD) Management

Enable Device Choice

- Support all operating systems and latest device models
- Enable employees to choose the most productive device

Enroll Devices Easily

- Enroll personal devices into AirWatch
- Select “Employee Owned” device ownership

Manage Personal Devices

- Configure policies and settings based on device ownership
- Secure access to enterprise resources, apps and documents

Protect Employee Privacy

- Configure what info is collected based on device ownership
- Isolate and protect both corporate and personal information

Mitigate Business Risks

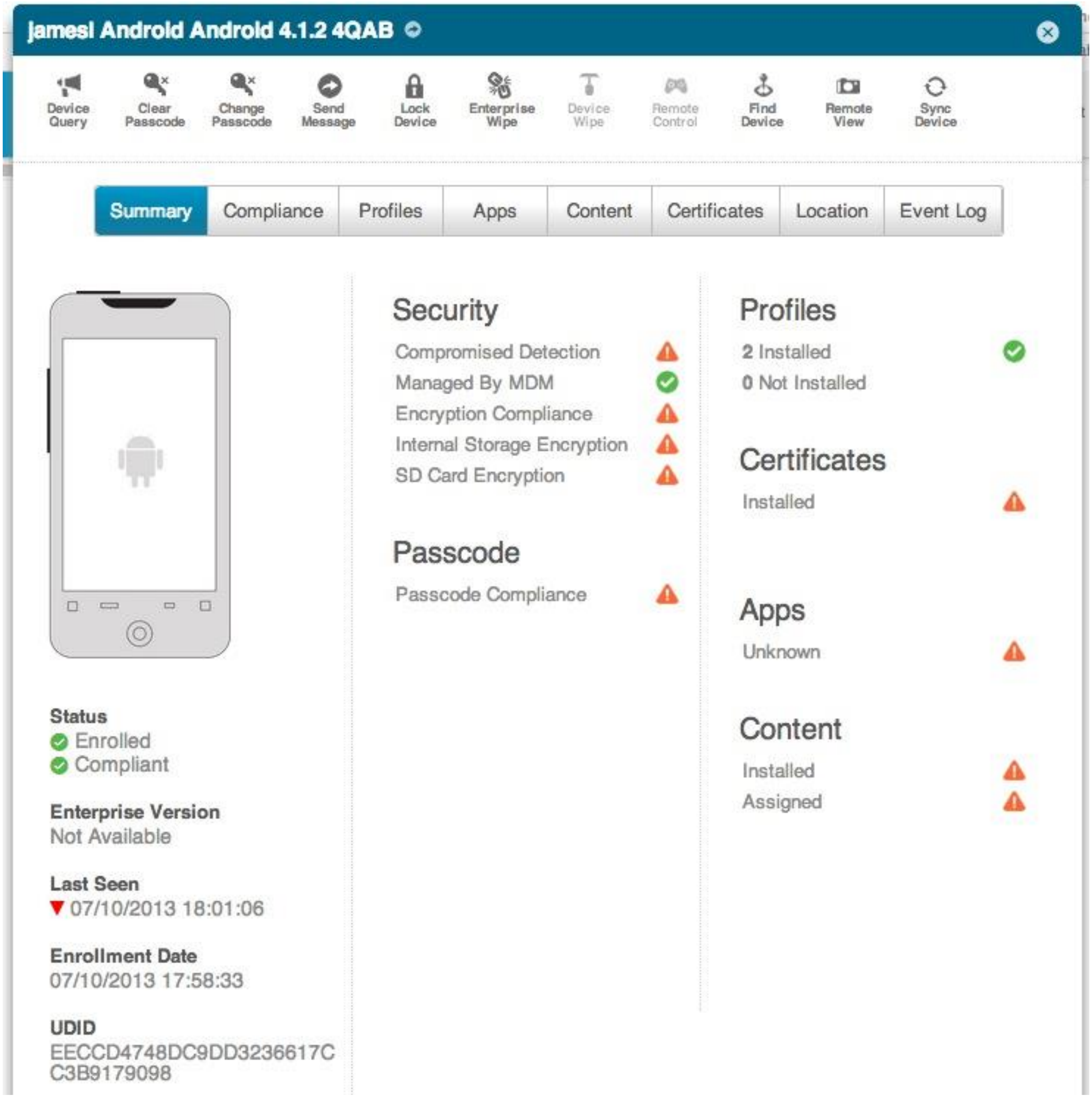
- Enforce custom Terms of Use agreements for employee devices
- Specify the info being collected and actions IT is allowed to take

Enable Self-service Management

- Simplify enrollment, configuration and support capabilities
- Locate, lock and perform an enterprise or full device wipe

6

In connecting via Airwatch, mobile device management is available via organisation specific console, providing assurance of security, apps, status and last connection /update to the corporate network.



jamesl Android Android 4.1.2 4QAB

Status
✓ Enrolled
✓ Compliant

Enterprise Version
Not Available

Last Seen
▼ 07/10/2013 18:01:06

Enrollment Date
07/10/2013 17:58:33

UDID
EECCD4748DC9DD3236617C
C3B9179098

Security

Compromised Detection	⚠
Managed By MDM	✓
Encryption Compliance	⚠
Internal Storage Encryption	⚠
SD Card Encryption	⚠

Passcode

Passcode Compliance	⚠

Profiles

2 Installed	✓
0 Not Installed	

Certificates

Installed	⚠

Apps

Unknown	⚠

Content

Installed	⚠
Assigned	⚠

Configuration specific to NHIS supported organisations has provided a MINIMUM criteria for the safe connection of devices ensuring that the configuration complies with organisational requirements and relevant UK Law. This MINUMIM criteria has been shared with all NHIS customers receiving Airwatch services. Enhancements to the MINIMUM are available, further details can be provided via the NHIS Business Relationships Team.

NHIS MINIMUM mobile device management set up – BYOD devices – Corporate bubble delivering Outlook content only.

Requirement	Provisioned	Managed	Assured
Secure Content Delivered	Yes	Group Policy : NHIS	Standard Reporting Template – available to nominated CCG User
Secure perimeter of Content	Yes	Group Policy: NHIS	Standard Reporting Template – available to nominated CCG User
Remote wipe / severance	Yes	Group Policy : NHIS	Standard Reporting Template – available to nominated CCG User
Password Reset enabled	Yes	Individual Option; Can be mandated by NHIS	Standard Reporting Template – available to nominated CCG User
GPS Tracking	No	Group Policy: NHIS Observance of Regulation of Investigatory Powers Act 2000	Standard Reporting Template – available to nominated CCG User

To request connection of a Personally Owned device – please go to

https://customerportal.notts-his.nhs.uk/

And select the option equipment, and BYOD Connection.

Appendix Two: Bring Your Own Device Application Form

Bring your Own Device Policy Statement

Please note that all of the requirements below must be agreed prior to any connection to the NHIS managed networks, as **a separate requirement** to those relating to behaviours as stated by the individuals' employing organisation.

NHIS have provided support for Airwatch **within existing Service Level Agreement Hours** – This means that any loss or compromise of devices outside of operational hours (Mon – Fri ,9 – 5 excluding public holidays), must be reported by the service user on the **next working day.**

Airwatch secures each device after 5 minutes of inactivity, minimising the risk of inappropriate access to corporate data, and this limitation is accepted by all customer organisations.

Your employing organisation has committed to supporting this process, by sharing HR starters and leavers' information. At the close of your employment, Airwatch will wipe content from your device. Please note that this **will** be enacted should your job role change within the NHS.

Requirement	**Agreed (Yes or No)**	**Signature of employee**
The mobile device remains your responsibility – NHIS will not undertake fix / maintenance / replacement of your device.		
The device must be as 'factory settings' – i.e. not 'Jalibroken' – to be clear: Jailbreaking increases the risk of malware infection or hacking. A jailbroken device can be easily victimized by a Trojan or accessed remotely by an intruder. Any security measures provided by iOS or installed third-party applications may be rendered inoperable or untrustworthy.		
The device must be included in the device listing of those which we can install Airwatch.	*For NHIS Confirmation*	
Airwatch will be installed on the device, and the cost of this is to be met by: the individual / employing organisation * (delete as appropriate), and this mandates and enforces a 6 digit passcode to be in place at all times.		
NHIS have the right to wipe the device if we feel that security / access is compromised.		
Should the user input the incorrect passcode		

in excess of the permitted number of attempts (10), Airwatch will automatically wipe the device.		
NHIS will take no responsibility for the loss / removal of any personal data held on the device associated with the operation of security on the device.		
If you lose your device then you must inform NHIS immediately – if this is outside of operational hours, then on the next working day.		

Employee Declaration

I (___________________) have read ad understood the Bring Your Own Device Policy Statement, and consent to adhere to the rules outlined.

I understand this is in addition to any policy of my employing organisation in regard to mobile device access and behaviours.

_____________________________________ _________________________________

Employee Signature Date

_____________________________________ _________________________________

Print Name

____

_____________________________________ _________________________________

Manager Signature Date

_____________________________________ _________________________________

Print Name

____

Managers Authorized Budget Code (agreed to be charged for Air watch license and annual support.)

____

_____________________________________ _________________________________

IT Admin Signature Date

_____________________________________ _________________________________

Print Name

____

END OF DOCUMENT