MobileCaddy Security Overview

Inc Cloud Control Matrix (Version 3.0.1)

Version 2.2

Last updated: June 2016

Index

Introduction

MobileCaddy (or the "Company") is a Salesforce certified ISV providing a 'managed package' Salesforce platform extension that is 'installed' via the Salesforce managed package/ISV installation process into Salesforce clients production or sandbox instances with System Administration security access. In Conjunction with the 'managed package' MobileCaddy provide 'Container Applications' that are installed on Customer's User Devices and download Application logic, interfaces and assets and synchronise and locally stores Customer Data directly from the Customer's Salesforce 'Instance(s)'.

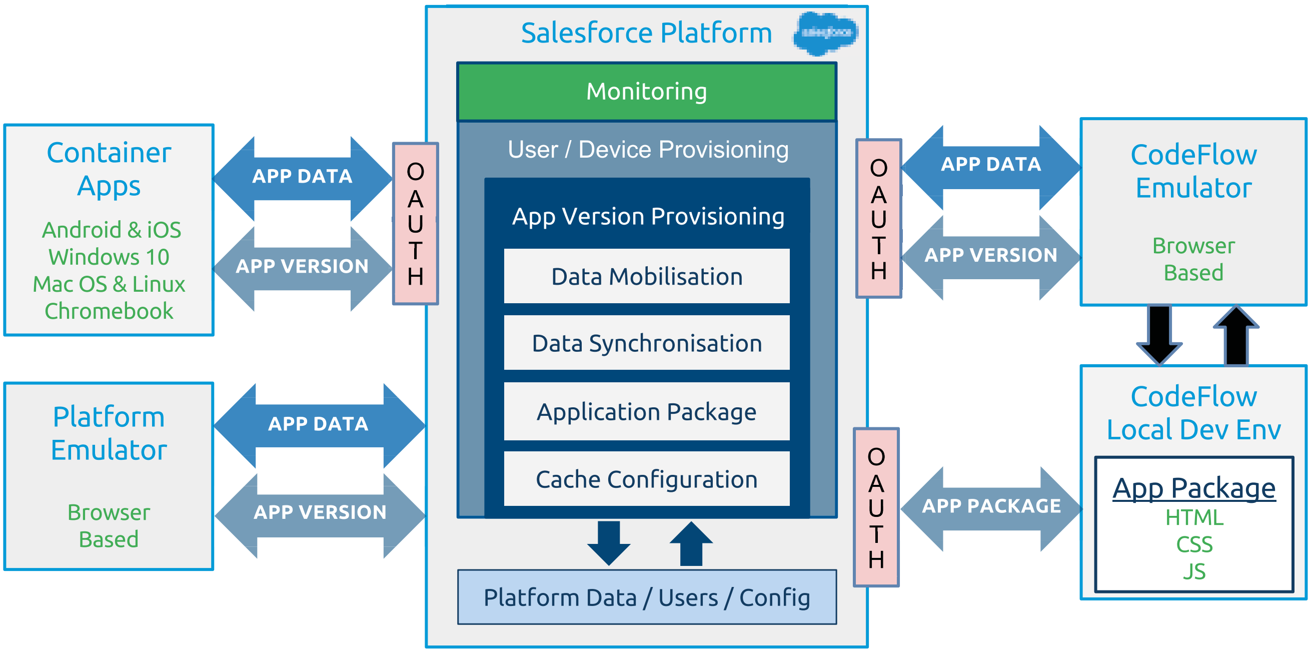
The MobileCaddy application provides Salesforce clients the ability to rapidly develop, transition, operate, support, monitor and improve, network resilient mobile applications that integrate with the Salesforce platform, specifically with the client's Salesforce 'instance(s)'.

The MobileCaddy application is native to the force.com platform and is regularly reviewed (at least annually) by the Salesforce.com review team including Security reviews, Platform rule adherence to sharing and data access, as well as integration testing for off-platform clients such as iOS and/or Android IPAs and APKs (ie client/device installables or 'Container Apps'). Details of the security review can be found here - http://sforce.co/2k71v38

Please note that this document is for informational purposes only. MobileCaddy has made every effort to provide responses that are accurate as of the date of publication. Because our procedures and policies change from time to time, we cannot guarantee that responses contained herein will be identical to those in our contracts. If you choose MobileCaddy as your provider, we will enter into contracts that cover many of the topics below, and those contracts will be definitive agreements.

The information provided in this document references services branded as Force.com, Database.com, Sales Cloud, Service Cloud, Communities, and Chatter (referred to hereafter as the "Salesforce Services"). The MobileCaddy managed package or application may be referred to interchangeably as "MobileCaddy Application", "MobileCaddy Managed Package" or "MobileCaddy Services".

MobileCaddy Architecture



MobileCaddy - Managed Package

The MobileCaddy package is developed using Salesforce proprietary technologies such as Apex (object-orientated programming language) and Visualforce (UI Framework). When the package is installed via the Salesforce package installation process a number of custom Salesforce sObjects and fields are created in the client's production or sandbox instances. All data that the MobileCaddy configuration creates is stored directly within the client's environment and is manageable via the standard or custom Sharing Models available Salesforce administration configuration.

Once the configuration process is complete the client/device applications will authenticate via the Salesforce oAuth 2.0 flow using user credential or a client provided SSO flow and retrieve and insert data directly to the client's Salesforce instance. All client data is stored, retrieved and inserted/updated directly via the Salesforce APIs. No 3rd party servers or data processing is used/utilised. All code and data interacted with is within the client's Salesforce instance.

MobileCaddy - Container Applications

The MobileCaddy container applications are built and maintained by MobileCaddy based off the Salesforce Mobile SDK technology (see more here). All locally stored data is encrypted at rest and data transfer is via HTTPS secure communication protocol encrypted by Transport Security Layer (TLS). All endpoints are Salesforce endpoints and communication requests via HTTP are denied by Salesforce servers (unless configured by the client's Salesforce Administrators)

Authentication

All components of a MobileCaddy Container Application require user authentication at the point and time of access unless specifically requested by the Customer. MobileCaddy Container Application utilises OAuth2.0 for authentication through Salesforce username/password or SSO (single sign-on) credentials.

OAuth Pairing

During the initial login, the device is uniquely identified and paired with the mobile user's account using the OAuth 2.0 protocol (http://tools.ietf.org/html/rfc6749). All requests to the Salesforce service are made using the OAuth token established through the pairing created during activation. After initial login, there is no exchange of a password in the communication between the mobile client and the Salesforce server. For this reason, the Salesforce password is not stored on the device and is not required even when the password is changed or has expired. A user obtains an access and refresh token after successfully completing the OAuth 2.0 web server authentication. A user can use the refresh token to get a new access token (session ID). Upon logout, the OAuth access and refresh tokens are revoked, and the user set passcode is wiped (if a passcode is developed in the local application code). The user is re-prompted to enter the username/password and reset the passcode. The org administrator can revoke a refresh token the first time a user uses the app, every time a user uses the app, or on set a schedule (hourly, daily, or monthly) to force a user to re-enter the username/password and reset the passcode. The default token expiration schedule is set at 2 hours, but can be as short as 15 minutes.

OAuth Refresh Token Storage

iOS Downloadable App: AES-128 with a 256 bit key consisting of a SHA-256 hashed concatenation of a generated RFC 4122 Universally Unique Identifier (persisted to the encrypted keychain). Token is stored in the keychain using kSecAttrAccessibleWhenUnlockedThisDeviceOnly.

Android Downloadable App: PBKDF2 produced AES-256 encrypted key derived from device unique Android ID and randomly generated string. Token is stored in Android's AccountManager. The SQLCipher-encrypted key is derived from the UUID (universally unique identifier).

Session Token

MobileCaddy Container Applications are all hybrid applications using Visualforce Salesforce technology. The Session Token is derived from the OAuth Access Token and is scoped to the Visualforce 'start page' defined in the Mobile Application version. The UIWebView/Webview stores it in the cache.

Single Sign On

Single sign-on is a process that allows network users to access all authorised network resources without having to log in separately to each resource. Single sign-on allows orgs to validate username/password against their user database or other client applications rather than having separate username/password managed by Salesforce. Note MobileCaddy cannot guarantee interoperability with all SSO implementations.

Please refer to SSO documentation at http://developer/mobilecaddy.net/docs/ and utilise configuration testing services.

> Federated Authentication Support
> When federated authentication is enabled, Salesforce doesn't validate a user's password. Instead, Salesforce verifies an assertion in the HTTP POST request, and allows single sign-on if the assertion is true. This is the default form of single sign-on.

> Delegated Authentication Support
> When delegated authentication is enabled, Salesforce does not validate a user's password. Instead, Salesforce makes a Web services call to a customer org to establish authentication credentials for the user. Customer's Administrators must request delegated authentication support be enabled by Salesforce.

Identity Providers and Service Providers

An identity provider is a trusted provider that enables a customer to use single sign-on to access other websites. A service provider is a website that hosts applications. Customers can enable Salesforce as an identity provider, then define one or more service providers, so their users can access other applications directly from Salesforce using single sign-on. This can be a great help to users: instead of having to remember many passwords, they will only have to remember one. Salesforce is automatically enabled as an identity provider when a domain is created. After a domain is deployed, administrators can add or change identity providers and increase security for their organization by customizing their domain's login policy. Enabling Salesforce as an identity provider requires a Salesforce certificate and key pair that is signed by an external certificate authority (CA-signed) or self-signed. If customers haven't generated a Salesforce certificate and key pair, one is automatically created for them when they enable Salesforce as an identity provider. They also have the option of picking an already generated certificate, or creating one. Salesforce uses the SAML 2.0 standard for single sign-on and generates SAML assertions when configured as an identity provider.

Device Local Storage

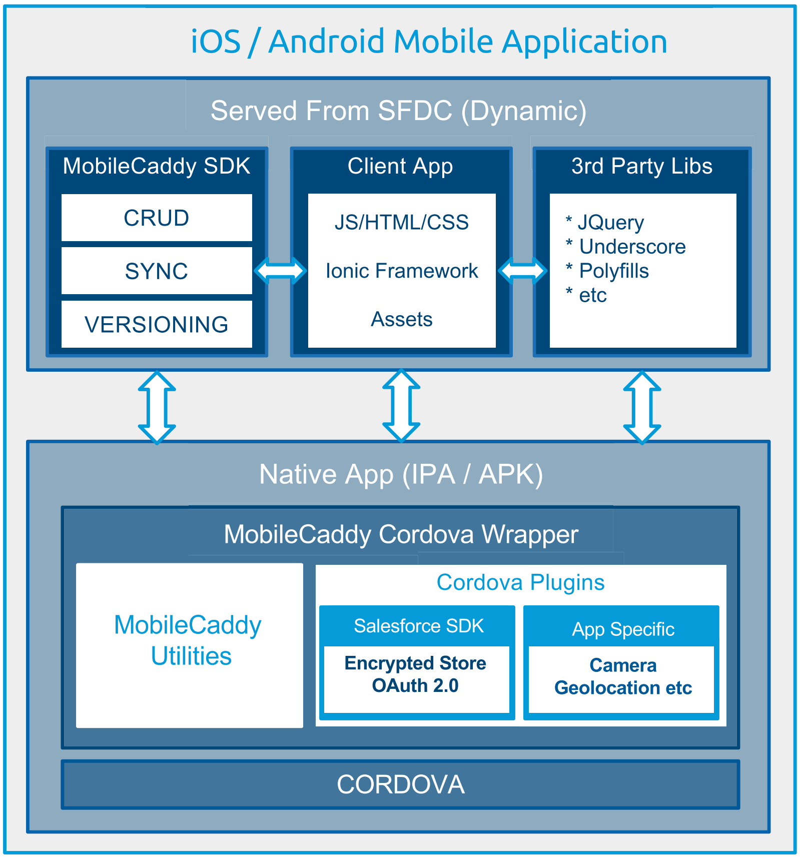
iOS Container Applications: Offline data is stored in the Salesforce Mobile SDK SmartStore, which is a SQLCipher-encrypted SQLite database with PBKDF2 produced AES-256 encrypted key in CBC (cipher-block chaining) mode with appropriate IV (initialization vector) and PKCS #5 padding.

Android Container Applications: Offline data is stored in the Salesforce Mobile SDK SmartStore, which is a SQLCipher-encrypted SQLite database with PBKDF2 produced AES-256 encrypted key in CBC (cipher-block chaining) mode with appropriate IV (initialization vector) and PKCS #5 padding.

Notes

MobileCaddy Container Applications in combination with the Salesforce platform and services provides multiple levels of security; however, there's no application that can guarantee a completely secure system.

MobileCaddy - Container Application Architecture



Salesforce Security Review

The Salesforce review ensures all Sharing, CRUD and FLS (field level security) is adhered to via the logged in User's Profile, Role and any OWD (organisation wide defaults) as well as meeting other criteria (see below) to ensure the Salesforce security policies and standards are adhered to (details below). The MobileCaddy transaction monitoring system (which is part of the installed package) creates logging of data and user transactions directly with the client's instance. Amongst other logs all attempts to access data (which will be denied by the Salesforce CRUD/FLS rules as defined by the client) will be logged and alerted internally if the client support team so chooses.

The Salesforce Security review covers:

Force.com Code

Single sign-on is a process that allows network users to access all authorised network resources without having to log in separately to each resource. Single sign-on allows orgs to validate username/password against their user database or other client applications rather than having separate username/password managed by Salesforce. Note MobileCaddy cannot guarantee interoperability with all SSO implementations.

Please refer to SSO documentation at http://developer/mobilecaddy.net/docs/ and utilise configuration testing services.

> Apex
>
> - Sharing: Use the “with sharing” keyword when declaring a class to respect sharing rules that apply to current users, unless there is a specific and valid business case to over-ride this which should be marked in false positive document.
>   - » Controllers retrieving user-specified objects as well as global classes must always use sharing.
>   - » Classes that modify standard fields must use sharing.
>   - » Classes that modify only custom fields owned by the partner and that are not entry points to the app may use without sharing if they prefer to enforce their own security controls rather than those of the platform.
>
> - CRUD and FLS: Enforce and respect FLS (Field Level Security) and CRUD (Create, Read, Update, Delete) settings configured by your customer’s org administrator when accessing fields that you do not own (standard fields).
>
> - Shield: Enforce the encryption model put in by shield by using Schema.sObjectType.Contact.fields.Phone.isEncrypted() and checking whether or not the user has the permission PermissionsViewEncryptedData.
>
> - Cross-Site Request Forgery in Visualforce pages: Avoid doing DML operations in page actions or in any action that runs automatically (e.g. javascript submitting forms on page load) Secure Coding Cross Site Request Forgery.
>   A possible work-around could be to insert an intermediate VisualForce confirmation page before taking the action, to make sure the user intended to call the page. Note that a Javascript based confirmation page can easily be bypassed and therefore is not effective.
>
> - Triggers: Ensure triggers are bulkified.
>
> - Metadata: If your package accesses metadata during installation or update, or contains a custom setup interface that accesses metadata, you must notify the user. The notice should let customers know that your package has the ability to modify the subscriber org’s metadata. For installs that access metadata, notify the user in the description of your package.
>
> - Tests: Use System.assert methods as much as possible to prove that code behaves properly.

> VisualForce
>
> Visualforce mergefields, will properly escape all string types based on the rendering context: In html text nodes, no escaping is necessary. Within script tags or javascript event handlers, mergefields should be wrapped with JSENCODE() and then quoted. Do not place mergefields that are of string type within style tags.
>
> - Do not place visualforce mergefields within client side micro templates (for example, angular templates). Assign quoted mergefield to a javascript variable within a script tag and then pass the variable to the compiled template or to the client side controller

Custom Javascript & HTML

- In order to prevent XSS attacks, the application must properly output encode data for the appropriate rendering operations (e.g. element.innerHTML=..., a.href=...).

- JavaScript that is part of partner offerings should not execute within the context of the Salesforce.com application. Partner JavaScript may only execute within the context of Visualforce. This means that any OnClickJavascript in custom buttons or weblinks is grounds for failure.

- All script and style resources must be loaded via static resources. Do not load resources dynamically with a link or script tag. Do not hotlink to javascript code outside of static resources.

- To aid in reviewing custom javascript, include un-minified source files when submitting for the security review corresponding to all minified files in static resources. Please give the unminified files the same name (except .min), for scanning purposes. Do not combine unminified and minified files together. Also include source files for all languages that transpile to javascript in your code (e.g. JSX). Auxiliary source files should be provided in static resources.

Storage of Sensitive Information

Ensure that sensitive information is not available to all users in a customer org. This can be achieved by using Custom Settings or Custom Metadata Types in “Protected” mode and creating a Visualforce page for authorized users to update information. The previously stored data should not be displayed back to the user on this page (define a null getter and also mark the variable as private and transient). Another option is to implement Apex Crypto and store the encryption key in a protected custom setting.

Client Applications

> Policies
> Implement an Information Security Policy that is periodically reviewed, approved by Senior Management, and communicated to all employees.

> Standards & Procedures
> - System Configuration
> - Application Development
> - Application Configuration
> - Database Configuration
> - Network Configuration (Including Firewall/IDS)
> - Patching Process
> - Logging Process/Log Review
> - Physical Security
> - Incident Management Process
> - Authentication & Authorization
> - Encryption Standard

> Host / Platform Security
> - Disable unnecessary services on key servers (web application, database, etc.)
> - Run up-to-date versions of all services on key servers.
> - Implement robust patch management
> - Remove/Rename default accounts and change default passwords
> - Securely hash all passwords with a unique, random salt
> - Create unique usernames for all users

- Implement a robust password policy (organizational and application)
  - » Minimum 8 characters
  - » Combination (2 out of 4) of numbers, letters (lower and upper) and special characters
  - » Enable lock outs for bad attempts (3-5)
  - » Enable password expiration (90-180 days)
  - » Enable password history (don't allow reuse of last 5 passwords)
  - » Passwords should not be sent to third parties (Google analytics, fullstory)
- Implement system logging and enforce periodic review of logs
- Implement host based firewalls on critical systems
- Implement secure remote access (VPN – SSHv2, SSL, IPSEC, or AES)
- Persistent tunnels configured with appropriate ACLs
- Implement an enterprise-wide anti-virus solution with daily updates
- Remote Desktop or Terminal Services Remote Administration should not be exposed to Internet facing connections.

Application Security

Reverse Proxy based apps are not allowed on the AppExchange.

- Implement a strong SDLC with security being a core component
  - » Implement code reviews
  - » Implement a testing/QA methodology
  - » Implement a methodology for rolling code to production
- Implement appropriate segregation of duties within the test, development and production environments
- Unless necessary, do not store salesforce.com credentials (leverage the Session IDs)
  - » If necessary, have a clear rationale and communicate this to salesforce.com
- Implement encryption in transmission and storage (login credentials and salesforce.com customer data)
  - » Support TLSv1.1 and newer versions
    - ◊ Strong configurations are also required. See https://www.ssllabs.com/ssltest/ for a security rating for your configuration
  - » Set "secure" flag on session cookies
  - » Do not store encryption keys in source code
  - » Implement encryption key management
- Prevent username enumeration
  - » Do not give different feedback to the user if the account does or does not exist in password reset pages
- Use CAPTCHA's or other defenses against automated login attempts
- Do not allow login CSRF (forced login)
- Avoid Dynamic SQL
  - » If Using Dynamic SQL, prepare appropriate rationale for salesforce.com
  - » Implement appropriate compensating controls
- Implement appropriate input validation and URL cleansing to prevent SQL Injection and Cross-Site Scripting (XSS) attacks
- All script and style resources must be loaded via static resources. Do not load resources with a link or script tag. Do not hotlink to js code outside of static resources.
- Ensure that Flash security recommendations are followed
- Implement controls to protect the Salesforce Session ID. Specifically:
  - » Session ID should always be encrypted in transmission
  - » Session ID should not be sent to third parties (Example: Google Analytics)
  - » Validate that the connection is being requested from a valid Salesforce server.

Operational Security

- Actively Monitor Network
- Implement and periodically test Disaster Recovery and Business Continuity Plans
- Implement an Employee Training and Security Awareness Program
- Implement Encryption Key and Privileged User Password Rotation
- Implement a robust change management process which includes documentation and approval of all changes
- Perform security review of third-party organizations

Enhanced Record, Object and Field Security for Mobile Applications

Above and beyond the Salesforce platform defined CRUD and FLS a client may choose to further restrict the read/write capabilities of any Mobile Application configured via the MobileCaddy managed package. This allows for Users access to be reduced when accessing via a Mobile Application.

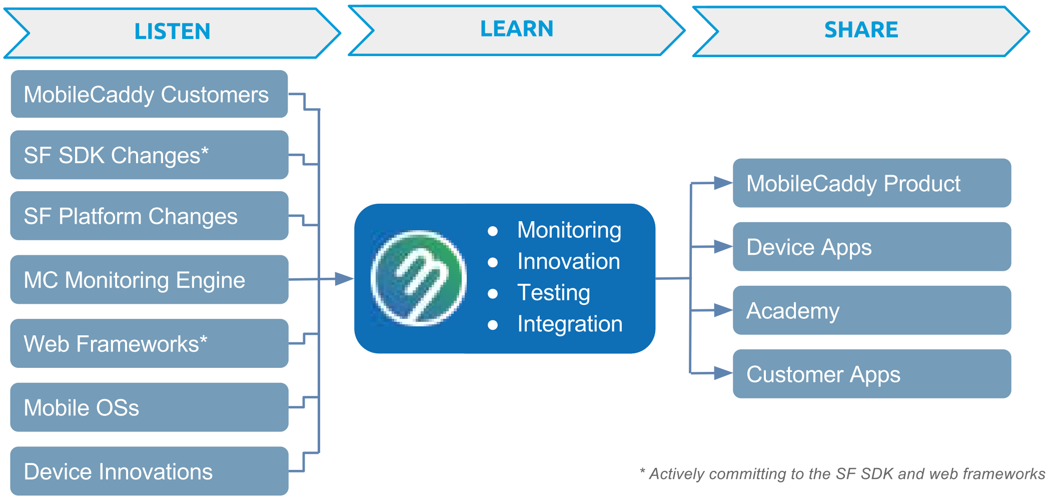
Mobile Application Data Recovery

To allow retrieval and recovery of data created or updated via the MobileCaddy Container Application and the Mobile Application code, MobileCaddy has three data recovery systems (in-app, remote and local). In all cases the recovery systems can only be entered via a Challenge/Response system. This involves a randomly generated Support PIN presented to the User when attempting to enter any of the recovery systems. This Support PIN then has to be validated against the Mobile User record on the Salesforce platform which creates a response PIN for the User to enter which then allows the recovery system to be accessed.

Customer Security Reviews and Audits

For customer security reviews and audits that the client may be obligated or choose to perform detailed are generated as described above for user transactions. The installed MobileCaddy package also retains a running ID list of record that are present on each user(s) device(s). This record will show sent (new), current (previously sent) and removing IDs.

Security Alerts and Notifications



Copyright MobileCaddy Ltd. All rights reserved.
Marks appearing herein may be trademarks of their respective owners.

MobileCaddy operate a continuous monitoring system that monitors the external environment (such as the Salesforce system and releases), Container App Operating Systems (such as iOS and Android) as well as transactional data (containing only logging data and failure codes with Org and User IDs to aid Customer notification).

This monitoring also covers security issues raised by external environment dependencies as well as the Salesforce Services which host the MobileCaddy Managed Package and Customer Data.

The monitoring system is checked daily with manual system tests to ensure maximum uptime.

Pre-release Security Testing

For each release of the Salesforce platform (Spring, Summer, Winter) MobileCaddy run manual and automated testing against a wide variety of org configurations and user profiles and roles and access levels. These are tested prior to Salesforce GA release covering pre-release production and sandbox early release.

For each version of Container App Operating Systems MobileCaddy test against a variety of emulated and physical devices.

Details of all issues including security issues are posted to http://trust.mobilecaddy.net

The Cloud Security Alliance's Cloud Control Matrix

In this document, MobileCaddy provides detailed information about how the Company and Salesforce where the MobileCaddy Managed Package is hosted and runs, helps fulfill the applicable security, privacy, compliance, and risk management requirements defined by the Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM). The CSA is a not-for-profit, member-driven organization of leading industry practitioners,with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. CSA is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. The CSA CCM is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security and privacy concepts and principles that are aligned to the Cloud Security Alliance guidance in 16 domains.

Control Area	Control ID	Control Specification	Control Notes
Application & Interface Security *Application Security*	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	MobileCaddy's Software Development Lifecycle (SDLC) processes are consistent with industry standards and follow internal SDLC requirements, which address applicable guidance (including Salesforce ISV certification requirements) to prevent vulnerabilities.
Application & Interface Security *Customer Access Requirements*	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	MobileCaddy is a native Salesforce ISV application and as such all Customer Data resides exclusively in the Salesforce Instances ("Orgs") included and made available by Salesforce to the Customer. Customer data submitted to the Salesforce Services by Salesforce's customers ("Customer Data") is managed by the customer in their use of the Salesforce Services. Customers are responsible for complying with applicable laws in using the Salesforce Services. All user and application level security controls are defined and maintained by the organisation administrator, and not by MobileCaddy or Salesforce. The organisation administrator is appointed by the customer. An organisation's sharing model sets the default access that users have to Customer Data.
Application & Interface Security *Data Integrity*	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Application logic enforces input by Customer Data type on the Salesforce platform and is further designed (but cannot increase in access) into the Mobile Applications as agreed by the Customer. It is the customer's responsibility for monitoring proper entry of Customer Data. The Salesforce platform offers many features to help ensure the capture of effective and relevant Customer Data. The system offers features such as validation rules with red-highlighted error messages, administrator-defined field picklists, field default values, required fields, and bubble help text on data entry screens. The Mobile Application can be configured or increased to adhere to these with custom UI submission and validation rules during input but they will be enforced/rejected via the API call and subsequent operations. Database changes for the Salesforce Services are committed only under appropriate transaction controls.

Control Area	Control ID	Control Specification	Control Notes
Application & Interface Security *Data Security / Integrity*	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	MobileCaddy has documented security policies and procedures aligning with the requirements for Salesforce ISV Certification. Salesforce, as the hosting provider, maintain the Customer's data security as per their policies and certified to ISO 27001 Connections to the environment for the Salesforce Services is only available over a secure channel (HTTPS) and data in transit is TLS encrypted via cryptographic controls using global step-up certificates, ensuring that users have a secure connection from their browsers and/or Mobile Applications to the Salesforce Services.
Audit Assurance & Compliance *Audit Planning*	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	The MobileCaddy managed package is installed and runs within the Customer's Salesforce Instance's (Orgs). Salesforce provides robust security and privacy protections for information submitted to the Salesforce Services ("Customer Data") based on internationally-recognized standards, such as the ISO 27001 standard. Salesforce regularly undergoes audits by independent third parties to test the security and privacy control framework for Salesforce Services, including: ISO 27001, SOC 1 (SSAE 16/ISAE 3402), SOC 2, SOC 3 (formerly SysTrust), PCI-DSS, and FedRAMP. Additional information about Salesforce's independent reviews and assessments is available at: http://trust.salesforce.com. The MobileCaddy Package and Container Apps are submitted and reviewed (at least annually) via the Salesforce Security review team and ISV program requirements.
Audit Assurance & Compliance *Independent Audits*	AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	The MobileCaddy managed package is installed and runs within the Customer's Salesforce Instance's (Orgs). Salesforce provides robust security and privacy protections for information submitted to the Salesforce Services ("Customer Data") based on internationally-recognized standards, such as the ISO 27001 standard. The MobileCaddy managed package is installed and runs within the Customer's Salesforce Instance's (Orgs). Salesforce provides robust security and privacy protections for information submitted to the Salesforce Services ("Customer Data") based on internationally-recognized standards, such as the ISO 27001 standard.

Control Area	Control ID	Control Specification	Control Notes
			Additional information about Salesforce's independent reviews and assessments is available at: http://trust.salesforce.com. The MobileCaddy Package and Container Apps are submitted and reviewed (at least annually) via the Salesforce Security review team and ISV program requirements.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	MobileCaddy has a control framework capturing regulatory requirements for assessment including legal requirement for Mobile Application submissions to the relevant stores where applicable. The framework is reviewed on a regular basis, once a year or more. In addition Salesforce has sets of control frameworks for the provision of the Salesforce Services.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities	Primarily the MobileCaddy package is tied to the uptime of the Salesforce Services for the client Instance (Org). Salesforce has developed a Business Continuity program applicable to the Salesforce Services, which is managed by their Business Continuity team. This program is overseen by senior management for each of the key functional areas within Salesforce, and is supported by their executive leadership at the highest level. In addition MobileCaddy have a Business Continuity plan which also includes continuity issue reporting directly to Salesforce to notify of dependent system issues.

Control Area	Control ID	Control Specification	Control Notes
		- Detailed recovery procedures, manual work-around, and reference information - Method for plan invocation	
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	MobileCaddy has a control framework capturing regulatory requirements for assessment including legal requirement for Mobile Application submissions to the relevant stores where applicable. The framework is reviewed on a regular basis, once a year or more. In "MobileCaddy business continuity plans are tested at least annually as are those performed by Salesforce that applicable to Salesforce Services. MobileCaddy has a security incident response process which also includes notification to Salesforce personnel if driven or affected by a dependent Salesforce Service. During a security incident, the process guides MobileCaddy personnel in management, communication, and resolution activities. Regular updates are provided to engaged parties (including customers where appropriate) until issue resolution and general alerts are also published on the MobileCaddy Trust site (http://trust.mobilecaddy.net) " addition Salesforce has sets of control frameworks for the provision of the Salesforce Services.
Business Continuity Management & Operational Resilience *Datacenter Utilities / Environmental Conditions*	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Being an installed managed package the MobileCaddy Services are tied to the the Salesforce Services which are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, the Salesforce Services have more than one piece of redundant equipment for a given function. The data center engineering staff provides 24-hour monitoring in the operations center for all critical components. Audits of security controls at the data centers used for the Salesforce Services are performed multiple times throughout the year for SOC 1 (SSAE 16), SOC 2, ISO 27001 and PCIDSS. Additionally MobileCaddy Container Apps are by design resilient to loss of connectivity which includes availability of the Customer Salesforce Instance (using a retain/retry model).

Control Area	Control ID	Control Specification	Control Notes
Business Continuity Management & Operational Resilience *Documentation*	BCR-04	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Standard operating procedures are documented and available for information systems supporting the MobileCaddy application documentation and for the Salesforce Services that host the application and Customer Data. Documentation is accessible on internal MobileCaddy and Salesforce intranet or wiki sites and restricted to personnel responsible for managing the system. MobileCaddy provides support case access and documentation to help resolve issues quickly as well as triage and diagnostic information through the use of Connection Sessions and Mobile Logs within a Customer's instance.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	The MobileCaddy package is 'installed' and run within an Customer Instance (Org) within a Salesforce data centre. When picking a data center location, physical protection against damage from natural causes and disasters, as well as deliberate attacks, are considered in the Salesforce evaluation criteria. Salesforce's data centers used for the Salesforce Services are located above sea level with no basement, dedicated pump rooms, drainage/evacuation systems and moisture detectors. The buildings are engineered for local seismic, storm, and flood risks. Data centers are in geographically disparate locations, so that a disaster at one data center would mean that the service fails over to a backup data center remote from the disaster area.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Some data centers for the Salesforce Services which host and run the MobileCaddy application may be located in locales with environmental risks, such as earthquakes, however additional precautions have been implemented to minimize the impact of such events. Please refer to the response provided to BCR-05 above for additional details.

Control Area	Control ID	Control Specification	Control Notes
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Maintenance of physical and environmental systems for the Salesforce Services which host and run the MobileCaddy application is performed in accordance to manufacturer specifications. These controls are tested for operating effectiveness during Salesforce's periodic third party compliance and audit activities.
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Please refer to the response provided to BCR-03 and BCR-05.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	MobileCaddy performs a Business Impact Assessment which includes the availability of the Salesforce Services. These primarily identify critical processes and services, dependencies, threats, and impacts resulting from disruption of the Salesforce Services and/or Container App or library failures, and establishes maximum tolerable period, priorities for recovery, and resources required. MobileCaddy performs monthly app recovery system tests using pre-configured environments matching Customers Salesforce platform configuration. These results feedback into updating the Continuity and Recovery processes and plans.

Control Area	Control ID	Control Specification	Control Notes
Business Continuity Management & Operational Resilience *Policy*	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Procedures are maintained by the Operations teams to ensure that consistent processes are followed in the management and support of the MobileCaddy application within the context of the Salesforce Services. These documents are available to all appropriate personnel required to perform Operations functions.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Retention: Salesforce's customers determine how long their respective Customer Data is retained in the Salesforce Services which host and run the MobileCaddy application. Customers may utilize the Salesforce Services' "Weekly Export" feature to export Customer Data and retain such information in separate systems. Backup: Customer Data is replicated to disk in near-real time at the designated secondary data center, and backed up at the primary and secondary data centers. Backups are performed daily at each data center facility without stopping access to the application. Replication is transmitted over an encrypted network. Disaster Recovery (Salesforce): The disaster recovery facilities for the Salesforce Services are geographically remote from primary data center facilities, with production-level hardware, software, and Internet connectivity. Salesforce has managed disaster recovery plans in place and tests them regularly. Disaster Recovery (MobileCaddy): The MobileCaddy package is installed within the client Salesforce instance (refer to above). The MobileCaddy disaster recovery extends to the Container Apps to allow for plans and recovery of specific user data in case of wider network failure.

Control Area	Control ID	Control Specification	Control Notes
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization’s business leadership or other accountable business role or function.	Salesforce has established policies and procedures for management authorisation for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities for the Salesforce application and services which host and run the MobileCaddy application and Customer Data.
Change Control & Configuration Management *Outsourced Development*	CCC-02	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Neither MobileCaddy or Salesforce which host and run the MobileCaddy application outsource software development for the MobileCaddy Application or Services or for the Salesforce Services.
Change Control & Configuration Management *Quality Testing*	CCC-03	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	New system components of the MobileCaddy Application are evaluated by architectural and operational teams, and are introduced following change management requirements and inline with the Salesforce Services release cycle with access to the pre-release partner & ISV environments. For servers, network devices, and databases these are maintained by Salesforce with baseline configurations consistent with industry-accepted system hardening guidelines that address known security vulnerabilities. Operating systems, upgrades, and applications are tested prior to acceptance. Salesforce implements a multipronged approach to help ensure the software released is secure. From initial ideas to release, Salesforce deploys several tools and processes in this regard. MobileCaddy application development follows software development lifecycle requirements to help ensure security in the development lifecycle, with participation in architecture reviews and secure coding best practices. The Salesforce ISV security review of the MobileCaddy managed package combines the use of code scanners and manual security testing.

Control Area	Control ID	Control Specification	Control Notes
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	MobileCaddy deploys security measures and monitoring solutions to help ensure MobileCaddy employees only use approved applications and tools. Administrative access to the packaging environment for the managed package prior to uploading to Salesforce Services is strictly controlled. Salesforce which hosts and runs the MobileCaddy application and Customer Data deploys security measures and monitoring solutions to help ensure Salesforce employees download only approved applications and tools. Administrative access to the environment for the Salesforce Services is strictly controlled. Critical hosts employ file integrity monitoring (FIM) to detect and alert on changes to their file systems.
Change Control & Configuration Management *Production Changes*	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	The MobileCaddy managed package is installed and runs on Salesforce Network and infrastructure. The change control procedures are required by Salesforce's Change Management Policy applicable to the Salesforce Services and include steps for testing, review, authorisation, communication and fallback procedures. All changes to the infrastructure components are tested in a dedicated environment using production class equipment before being deployed into production. An emergency change process is also in place. Changes are reviewed and approved by Operations management prior to deployment to production for the Salesforce Services. System changes and maintenance are managed using a Salesforce internal case tracking system with Salesforce partner and ISV alerts. Salesforce vendor-supplied OS, application, and networking patches are evaluated by Salesforce systems administrators, tested on internal systems, and are deployed by the Salesforce Operations team during announced maintenance periods. MobileCaddy managed package uses a partitioned class approach allowing package upgrade and roll-back within production instances without impacting running client applications and allowing for client sandbox pre-release testing and managed roll-out.

Control Area	Control ID	Control Specification	Control Notes
Data Security & Information Lifecycle Management *Classification*	DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	MobileCaddy is hosted on Salesforce and generally does not have access or visibility into the types of information customers host within the Salesforce Services.
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	MobileCaddy does not have access or visibility into the data stored within the Salesforce Services.
Data Security & Information Lifecycle Management *Ecommerce Transactions*	DSI-03	Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	The MobileCaddy application is not an eCommerce solution; however eCommerce solutions may be built on the Salesforce platform by customers and partners and this Customer Data may be configured to be processed by the MobileCaddy managed package. Customer Data transmitted over the wire is secured using TLS 1.2 or higher and encrypted using 256 or 128-bit encryption. The Services use International/Global Step Up SSL certificates with 2048-bit Public Keys.

Control Area	Control ID	Control Specification	Control Notes
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Please refer to the response provided to DSI-01 above.
Data Security & Information Lifecycle Management *Non-Production Data*	DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	MobileCaddy has no access or visibilty to Customer Data.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	MobileCaddy's customers retain all ownership rights to their respective Customer Data.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Utilising the MobileCaddy package installed on the Customer Salesforce Instance (Org) Customer Data submitted to the Salesforce Services remains on disk until the customer deletes or updates it. Customer Data deleted by a customer is temporarily available within a "recycle bin" before being deleted from the system. MobileCaddy has no access or visibility to Customer Data.

Control Area	Control ID	Control Specification	Control Notes
Datacenter Security *Asset Management*	DCS-01	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Asset management is defined through the company's Information Systems Asset Management Policy. This covers items such as acquisition, tracking, ownership, responsibilities and disposal.
Datacenter Security *Controlled Access Points*	DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	MobileCaddy is a managed package that is installed via Customer System Administrators and hosted by Salesforce. The Salesforce data centers are physically secured using a defense in depth approach. Access to Salesforce data centers is authorised based on position or role and limited to those few individuals with a business need. Access is controlled via badges/pin pads, biometrics, and security guards. Subsequent entry to the production rooms and cage areas requires two-factor access, including biometrics.
Datacenter Security *Equipment Indentification*	DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Salesforce controls access to the Salesforce Services' infrastructure which host the MobileCaddy application and Customer Data, and these infrastructure components are physically and logically controlled by Salesforce staff. Please also refer to the response in DCS-02.
Datacenter Security *Off-Site Authorization*	DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	MobileCaddy is a managed package that is installed via Customer System Administrators and hosted by Salesforce. Salesforce require authorisation prior to relocation or transfer of hardware, software, or Customer Data of the Salesforce Services to an offsite premise. Customer Data is kept in Salesforce's secure, dedicated data center space until the systems containing Customer Data are to be retired and destroyed. MobileCaddy has no access or visibility to Customer Data.

Control Area	Control ID	Control Specification	Control Notes
Datacenter Security *Off-Site Equipment*	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	MobileCaddy is a managed package that is installed via Customer System Administrators and hosted by Salesforce. Customer Data (and the hardware and software in which it resides) submitted to the Salesforce Services is never physically removed from data centers. Customer Data is stored in Salesforce's secure data center facilities. Salesforce sanitizes media that contain Customer Data prior to disposal following the NIST SP 800-88 Guidelines for Media Sanitization.
Datacenter Security *Policy*	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	MobileCaddy is a managed package that is installed via Customer System Administrators and hosted by Salesforce. MobileCaddy does not run, own or have access to physical data centres housing Customer Data.Salesforce has established policies and procedures that govern their offices and data centers for the Salesforce Services. Salesforce implements physical security measures to protect the data centers for the Salesforce Services from unauthorised access and intrusion. Access to these data centers is limited to those personnel who require such access to perform their current duties. Hardware and infrastructure supporting the Salesforce Services are managed by full-time Salesforce employees only. Access is controlled via badges, biometrics, and security guards. Data center physical security is covered in Salesforce's SOC 1 and SOC 2 Type II reports, which are performed twice annually. The reports are available upon request under NDA.
Datacenter Security *Secure Area Authorization*	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	MobileCaddy is a managed package that is installed via Customer System Administrators and hosted by Salesforce. MobileCaddy does not run, own or have access to physical data centres housing Customer Data. Data centers for the Salesforce Services which host and run the MobileCaddy application and Customer Data are physically secured using a defense in depth approach. Access to these data centers is authorised based on position or role and strictly limited to individuals with a business need. Access is controlled via badges/pin pads, biometrics, and security guards. Subsequent entry to the dedicated Salesforce production data center cages/computer rooms requires two-factor authentication (a pin pad or badge and biometric access).

Control Area	Control ID	Control Specification	Control Notes
Datacenter Security *Unauthorized Persons Entry*	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	MobileCaddy is a managed package that is installed via Customer System Administrators and hosted by Salesforce. MobileCaddy does not run, own or have access to physical data centres housing Customer Data. Physical access to the data centers and server rooms for the Salesforce Services which host and run the MobileCaddy application and Customer Data are monitored 24/7 by data center security personnel through guarded lobbies and CCTV cameras set up inside and outside the data centers in critical areas. The critical areas monitored include; doors to colocation areas, access to cage or Salesforce computer room doors, server floor areas, external building perimeter, data center entries and exits, and shipping/ receiving areas. Salesforce controls visitor access (individuals without pre-authorised access) to the data center facilities by authenticating visitors before authorising access to the facilities. All visitors must be accompanied by an individual on the Salesforce authorised data center access list. Unaccompanied visitors are not allowed access to the data center. Upon arrival visitors must sign in at the front desk, submit a valid government-issued photo ID, and be approved by an individual on the Salesforce authorised list.
Datacenter Security *User Access*	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	MobileCaddy is a managed package that is installed via Customer System Administrators and hosted by Salesforce. MobileCaddy does not run, own or have access to physical data centres housing Customer Data. Please refer to the responses provided to DCS-07 and DCS-08 above.
Encryption & Key Management *Entitlement*	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	When a customer chooses to implement the Classic Encryption feature for Salesforce Services where the MobileCaddy package is hosted and runs, the application automatically creates a unique Customer encryption key for the exclusive use of that customer org.
Encryption & Key Management *Key Generation*	EKM-02	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and	The MobileCaddy package is hosted and runs on the Salesforce Services who manage encryption keys on behalf of customers. Key management and rotation procedures are in place to maintain keys for transmission and storage of Customer Data. Salesforce features enable customers to control their own keys and certificates for integrations with external systems.

Control Area	Control ID	Control Specification	Control Notes
		replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	
Encryption & Key Management *Sensitive Data Protection*	EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Database backups for the Salesforce Services, where the MobileCaddy package is hosted, are encrypted. Customers can optionally encrypt custom fields of specific types containing Customer Data which they deem sensitive. Using the Platform Encryption2 feature, customers can also encrypt a specific set of standard fields, files and attachments in their use of the Salesforce Services. Customer Data transmitted over the wire is secured using TLS 1.2 or higher and encrypted using 256 or 128-bit encryption. The Salesforce Services use International/Global Step Up SSL certificates with 2048-bit Public Keys.
Encryption & Key Management *Storage and Access*	EKM-04	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Customer Data transmitted over the wire is secured using TLS 1.2 or higher and encrypted using 256 or 128-bit encryption.

Control Area	Control ID	Control Specification	Control Notes
Governance and Risk Management *Baseline Requirements*	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	MobileCaddy has a formal process for placing a system into the production environment for the MobileCaddy application. This procedure includes a build checklist and pre-production testing. Baseline security standards are established by Salesforce's ISV certification for ISV managed packages such as MobileCaddy, which are applied during this process. Prior to releasing the managed package, management approval is required and the decision is based upon the results of the pre-production testing. MobileCaddy regularly reviews and works to improve its own security baseline requirements as well as those required by the Salesforce ISV package certification process. The Customer can choose to optionally install the managed package upgrade through managed package version system provided the Salesforce Services. This can be first deployed to a staging environment (Sandbox).
Governance and Risk Management *Data Focus Risk Assessments*	GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Regular risk assessments are conducted on an annual basis to evaluate risks to the Company's business, including potential loss, unauthorised access to, or misuse of Customer Data submitted to the Salesforce Services where the MobileCaddy package is hosted and runs. Customers determine how long their respective Customer Data is retained in the Salesforce Services and therefore the MobileCaddy managed package. Customer Data remains on disk until the customer deletes or updates it. Customer Data deleted by a customer is temporarily available within a "recycle bin" before being deleted from the system. Salesforce has defined retention periods and end-of-life disposal requirements. When production tapes for the Salesforce Services reach end-of-life, they are degaussed and destroyed. Hard drives are securely wiped before they are returned to the vendor. If hard drives cannot be overwritten, they are purchased and securely destroyed. MobileCaddy does not run, own or have access to physical data centres housing Customer Data.

Control Area	Control ID	Control Specification	Control Notes
Governance and Risk Management *Management Oversight*	GRM-03	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	All employees are required to acknowledge responsibility for complying with Company policies, including specifically Information Security policies.
Governance and Risk Management *Management Program*	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	MobileCaddy has developed Information Security Policies that acknowledge and record the risks, organisation and access specific and aligned to the Salesforce Services Security Management System. These are implemented and reviewed by senior management internally and at change points related to new and amended Security requirements of the ISV program so far as MobileCaddy does not run, own or have access to physical data centres housing Customer Data.
Governance and Risk Management *Management Support / Involvement*	GRM-05	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Please refer to the responses provided to GRM-02 and GRM-03 above.

Control Area	Control ID	Control Specification	Control Notes
Governance and Risk Management *Policy*	GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Information security policies are published on the Intranet and communicated to personnel through internal training and awareness campaigns. Regular required training on Information Security policies is conducted for all relevant staff. Please refer to the response provided to GRM-03 above.
Governance and Risk Management *Policy Enforcement*	GRM-07	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	MobileCaddy's information security policies contain enforcement sections providing that violations may result in disciplinary action up to and including termination.
Governance and Risk Management *Policy Impact on Risk Assessments*	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Security policies and procedures are reviewed a minimum of annually and updated if necessary. Security policies and procedures may also change in the event of a significant change in practice and/or a change the Saleforce ISV certification process as required for managed packages.
Governance and Risk Management *Policy Reviews*	GRM-09	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness,	MobileCaddy regularly reviews and improves its Information Security Management System manual and related policies applicable to the MobileCaddy Application. Individual policy documents are reviewed when revised or annually at a minimum if there are no revisions.

Control Area	Control ID	Control Specification	Control Notes
		accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	
Governance and Risk Management *Risk Assessments*	GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Company-wide risk assessments are performed annually to determine the likelihood and impact of identified risks. Results are contributed to the annual Internal Audit plan.
Governance and Risk Management *Risk Management Framework*	GRM-11	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Risk treatment plans state risk mitigation requirements, timelines, and organizational responsibilities. Risk acceptance is based upon recommendation by technical and compliance teams and requires senior management signoff.
Human Resources *Asset Returns*	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	MobileCaddy has a defined and documented process for the return of company-owned assets upon employment, contract or agreement termination.
Human Resources *Background Screening*	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to	The MobileCaddy Application is run and hosted on Salesforce infrastructure and services. No MobileCaddy employee has access to Customer Data or supporting Salesforce Services that may require access. Salesforce utilises a third-party provider to perform background investigations on all incoming employees in

Control Area	Control ID	Control Specification	Control Notes
		background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	the U.S. Salesforce also uses a third-party provider to perform background investigations on incoming employees in certain foreign countries. The scope of these checks is subject to local laws in the jurisdictions in which the employee is hired. Such investigations may include criminal background checks, education verification, and employment history verification.
Human Resources *Employment Agreements*	HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	MobileCaddy requires all employees to certify compliance with the Company's Code of Conduct, which includes sections on confidentiality, security, and privacy on an annual basis. MobileCaddy communicates on an ongoing basis with all employees regarding information security and privacy issues.
Human Resources *Employment Termination*	HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Roles and responsibilities for performing employment termination or change in employment procedures are managed and documented by the Company's Human Resources function. Violations of the Company's Code of Conduct, which includes sections on confidentiality, security, and privacy, may result in disciplinary action up to and including termination.
Human Resources *Mobile Device Management*	HRS-05	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Customer Data submitted to the Salesforce Services where the MobileCaddy managed package is hosted and run is not accessible by MobileCaddy employees or representatives. In relation to the Customer Data that is submitted directly to the Salesforce Services this is not stored on portable or mobile devices and technical controls are in place to prevent the transfer of Customer Data to portable media by users with logical access to manage the production systems. Salesforce has a comprehensive information security program that includes policies and procedures regarding portable and mobile devices, including the use of Mobile Device Management (MDM) technology. Information security policies are included within the scope of annual testing by Salesforce nominated external third-party auditor as part of the Salesforce's ISO 27001 certification.

Control Area	Control ID	Control Specification	Control Notes
Human Resources *Non-Disclosure Agreements*	HRS-06	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Requirements for confidentiality agreements reflecting the organisation's needs for the protection of data and operational details are identified, documented and reviewed at planned intervals.
Human Resources *Roles / Responsibilities*	HRS-07	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	MobileCaddy operates under a formal ISV commercial and operational agreement with Salesforce. All information assets and the security of Customer Data in relation to the Salesforce Services where the MobileCaddy Application will be hosted and run will be in accordance to the contracts in place for third parties supporting the Salesforce Services, which are issued, reviewed and maintained by Salesforce directly. Please also refer to the response provided to HRS-03.
Human Resources *Technology Acceptable Use*	HRS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	The confidentiality of Customer Data is of paramount concern to the Company and also it's obligation and requirements to meet and pass the Salesforce ISV security review requirements. Salesforce provides contractual assurance to its customers that the data customers host in the Salesforce Services will be kept confidential and not accessed except under narrow circumstances as set forth by contract (such as a support issue). Neither MobileCaddy or Salesforce claims ownership rights to Customer Data and Customer Data is only utilised as the customer instructs to either MobileCaddy or Salesforce, or to fulfill contractual or legal obligations. Additional information can be found on the Salesforces public facing trust website at https://trust.salesforce.com/ and the MobileCaddy public facing trust website http://trust.mobilecaddy.net/ Please also refer to the response provided to HRS-06 above.

Control Area	Control ID	Control Specification	Control Notes
Human Resources *Training / Awareness*	HRS-09	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	MobileCaddy requires every new hire to complete information security awareness training. The Information security policies are published on the Intranet and communicated to personnel through internal training and awareness campaigns on an ongoing basis.
Human Resources *User Responsibility*	HRS-10	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	MobileCaddy requires every new hire to complete information security awareness training. Training and awareness topics include the responsibility to follow Information Security policies including preventing unauthorised access to information.
Human Resources *User Responsibility*	HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	MobileCaddy has a Clean Workspace Policy that specifies protection of data in work environment including screen lock requirements based on inactivity as well as centralised control over automated session timeouts.

Control Area	Control ID	Control Specification	Control Notes
Identity & Access Management *Audit Tools Access*	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	MobileCaddy restricts, logs, and monitors access to its information security management systems for the Mobile Application monitoring systems. Log information is restricted to record IDs, error codes and Org Ids (full information is available at http://trust.mobilecaddy.net/security/). Access is restricted to a limited number of authorised personnel. The MobileCaddy managed packaged is hosted and runs on the Salesforce Services. MobileCaddy employees do not have access or visibility to these services. Salesforce as the hosting provider restricts, logs, and monitors access to its information security management systems for the Salesforce Services. Access to log data is restricted to a limited number of authorised Salesforce personnel. Segregation of duties are in place to ensure that individuals with access to logs are separate from operations teams.
Identity & Access Management *Credential Lifecycle / Provision Management*	IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)	The MobileCaddy managed packaged is hosted and runs on the Salesforce Services. MobileCaddy employees do not have access or visibility to these services. Salesforce's information security policies for the Salesforce Services contain access control sections based on the leastprivilege principle. A formal process is in place to request access to applications, databases, and server and network infrastructure supporting the Salesforce Services. All access requests must be approved by management, documented and periodically reviewed for appropriateness. Revocation of Salesforce user access is performed in a timely manner upon termination or transfer into a role that no longer requires existing access. Customer access to their Customer Data stored within the Salesforce Services which is created and/or processed by the MobileCaddy managed package is managed by the customer's application administrator(s). Salesforce offers a Security Implementation Guide that describes the controls and features available to application administrators within the service: http://resources.docs.salesforce.com/198/0/enus/sfdc/pdf/salesforce_security_impl_guide.pdf Refer to Salesforce's Multi-tenant Architecture whitepaper for information regarding access and logical data segmentation within the infrastructure: https://developer.salesforce.com/page/Multi_Tenant_Architecture

Control Area	Control ID	Control Specification	Control Notes
		• Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	

Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	MobileCaddy provides no infrastructure as the MobileCaddy managed package is hosted and run on Salesforce Services. Salesforce has internally-developed guidelines for hardening systems related to the Salesforce Services. All unused services, ports, and packages are disabled. Devices are configured to not expose management interfaces externally to the internet. A minimal set of user accounts is maintained and no shared password files are allowed. User access to systems supporting the Salesforce Services is restricted based on the least privilege principle.
Identity & Access Management *Policies and Procedures*	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Please refer to the response for Server Administrative Access in the IAM-02 Credential Lifecycle and Provision Management response above.
Identity & Access Management *Segregation of Duties*	IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Segregation of duties for the MobileCaddy Application is defined in the Company’s Segregation of Duties Standard which covers items such as ensuring pre-packaging administrators do not normally have access to the final packaging environment. Once the managed package is made available on Salesforce Services then the Segregation of duties for the Salesforce Services is defined in the Salesforce’s Segregation of Duties Standard which covers items such as ensuring administrators to one domain do not normally have access to other domains and the controls in place to grant, supervise and monitor such access. Salesforce developers do not have access to make changes to the infrastructure supporting the Salesforce Services. This is tested twice annually as part of Salesforce’s SOC 1 and SOC 2 Type II audits.
Identity & Access Management *Source Code Access Restriction*	IAM-06	Access to the organization’s own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	MobileCaddy have controls are in place to prevent unauthorised access to the packaging environment, program and object sources code for the MobileCaddy Application. Access is restricted to authorised personnel only and is audited regularly (at least annually). Salesforce have controls in place to prevent unauthorised access to the application, program and object source code for the Salesforce Services where the MobileCaddy application will be hosted and run. Access is restricted to authorised personnel only.

Control Area	Control ID	Control Specification	Control Notes
			This is tested twice annually as part of Salesforce's SOC 1 and SOC 2 Type II audits. Salesforce allows their customers to configure access to their instances of the Salesforce Services. This enables customers to restrict access to their Customer Data as they deem necessary. Beyond this the MobileCaddy managed package can be configured by the Customers System Administrators to further restrict access.
Identity & Access Management *Third Party Access*	IAM-07	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Access to the packaging and source code by third parties is covered by the overall risk assessment process for the MobileCaddy Application. It is not normal for third parties to require or be authorised for access. If it is deemed necessary MobileCaddy qualifies these parties following MobileCaddy's internal standards. Identification and prioritisation of risks due to access by third parties is part of Salesforce's overall risk assessment process for the Salesforce Services. Salesforce qualifies such vendors prior to access following the Salesforce's internal standards, including network and host controls, external scanning, and onsite audits and reviews of controls and documentation.
Identity & Access Management *Trusted Sources*	IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Please refer to the response for Server Administrative Access in the IAM-02 Credential Lifecycle and Provision Management response above.
Identity & Access Management *User Access Authorization*	IAM-09	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures.	The MobileCaddy information security policy stipulates access control based on the least-privilege principle. Access to the packaging environment and code repositories for the MobileCaddy Application is restricted to authorised personnel based on job function and requires documented management approval. Salesforce's information security policies for the Salesforce Services where the MobileCaddy managed package is hosted and run, contain access control sections based on the least-privilege principle.

Control Area	Control ID	Control Specification	Control Notes
		Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Access to production operating systems and databases and code repository for the Salesforce Services is restricted to authorised personnel based on job function and requires documented management approval. All users and application-level security are defined and maintained by a customer's organization administrator, and not by MobileCaddy or Salesforce. The organisation administrator is appointed by the customer. An organisation's sharing model sets the default access that users have to each other's data which can then be further enhanced by the MobileCaddy configuration at the field or object level. Please also refer to the response provided to HRS-08 above.
Identity & Access Management *User Access Reviews*	IAM-10	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	MobileCaddy conducts regular access reviews for Salesforce personnel with access to the MobileCaddy Application and packaging environments. The MobileCaddy senior management team reviews access regularly and at defined trigger points such as employee joiners and leavers. The MobileCaddy managed is installed and run on Salesforce Services. Salesforce conducts regular access reviews for Salesforce personnel with access to the Salesforce Services. Salesforce performs quarterly reviews for access to systems containing sensitive information. Such reviews are tested twice-annually as part of Salesforce's independent SOC 1 and SOC 2 Type II audits.
Identity & Access Management *User Access Revocation*	IAM-11	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant)	MobileCaddy's information security policies contain access de-provisioning sections. Access to packaging environments and code repository for the MobileCaddy Application is revoked upon notification of an employee's termination and ends on the date of termination. All users and application-level security are defined and maintained by a customer's organization administrator, and not by Salesforce or by MobileCaddy. The organisation administrator is appointed by the customer. An organisation's sharing model sets the default access that users have to each other's data. Salesforce provides tools for automated user de-provisioning and access revocation. Administrators appointed by customers can define and configure this process.The MobileCaddy package contains auto-provisioning of users which are de-provisioned automatically on the de-provisioning and access revocation of the Customer's Salesforce Users.

Control Area	Control ID	Control Specification	Control Notes
		data is used as part the service and/ or customer (tenant) has some shared responsibility over implementation of control.	
Identity & Access Management *User ID Credentials*	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/ multi-factor, expireable, non-shared authentication secrets)	User management and application-level security settings for the Salesforce Services where the MobileCaddy package is hosted and run are configured and maintained by the customer's administrator. These security controls include password strength (minimum length, complexity, aging, history), lockout after invalid attempts, identity verification prior to password reset, and session inactivity and duration limits. Customers can choose to implement stronger controls, such as SSO, IP address restrictions, and two-factor authentication using third-party packages, or via federated or delegated methods supported by the Salesforce Services, as needed. Customer administrators manage API accounts and their permissions in accessing the Salesforce Services. Equal or stronger controls are in place for Salesforce personnel provisioning the Salesforce Services. Refer to the prior responses for the Identity & Access Management control objective above for details on credential lifecycle management.
Identity & Access Management *Utility Programs Access*	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	The MobileCaddy package is hosted and run on the Salesforce Services. Salesforce has system hardening guidelines applied to servers, databases and network devices for the Salesforce Services. This includes the use of common configuration files to help ensure that the same services are disabled on all machines. In addition, Salesforce has File Integrity Monitoring installed on critical hosts supporting the Salesforce Services and monitor to detect and alert in the event that changes are made to critical system files and configurations. Salesforce does not utilize virtualization in the provision of the Salesforce Services.

Control Area	Control ID	Control Specification	Control Notes
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	The MobileCaddy package is hosted and run on the Salesforce Services and infrastructure. Privileged user access/failed attempts to Salesforce infrastructure, file integrity monitoring on hosts, and network intrusion detection events are logged and correlated in a security event monitoring system. Correlated events are configured to generate alerts and logs which are monitored by Salesforce's Computer Security Incident Response Team (CSIRT). As a component of Salesforce Shield3, Salesforce provides the complete application event logs to customers on demand. Customers can mine these logs and generate reports and visualizations as required by their policies.
Infrastructure & Virtualization Security *Visualization Security Change Detection*	IVS-02	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Not applicable. The Salesforce Services that host and run the MobileCaddy managed package do not utilize virtualization in the provision of the Salesforce Services.
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Clocks for routers, firewalls, and servers for the Salesforce Services that host and run the MobileCaddy managed package are synchronized using NTP, with the GPS clock as source.

Control Area	Control ID	Control Specification	Control Notes
Infrastructure & Virtualization Security *Information System Documentation*	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	The Salesforce Services which host and run the MobileCaddy managed package application are designed to achieve in excess of 99.9% availability. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Live and historical statistics on the Salesforce system performance is publicly published at http://trust.salesforce.com/trust/status. Salesforce has defined thresholds for key system components for the Salesforce Services, such as network, storage, memory, I/O, etc., which are monitored by Salesforce personnel. Capacity demands (system and application) are monitored daily. Capacity planning engineers monitor network, data center, infrastructure, and application utilization to ensure capacity demands are met, and future requirements are anticipated. The MobileCaddy Container application are designed for network resilience which includes end-point unavailability and employ a retain/retry model allowing for continuous operation for Container Application and seamless resumption as Services become available.
Infrastructure & Virtualization Security *Vulnerability Management*	IVS-05	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Not applicable. The Salesforce Services that host and run the MobileCaddy managed package do not utilize virtualization in the provision of the Salesforce Services.
Infrastructure & Virtualization Security *Network Security*	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.	Salesforce's network configuration standards for the Salesforce Services which host and run the MobileCaddy manage package, require network device rulesets to control connections to untrusted networks, and include allowed ports, protocols, and services, as well as a review of those rulesets at regular intervals. Network and data flow diagrams are regularly updated and reviewed as part of Salesforce Services' compliance audits.

Control Area	Control ID	Control Specification	Control Notes
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	The MobileCaddy managed package is hosted and run on Salesforce Services and infrastructure. Salesforce has a formal process for placing a system into production for the Salesforce Services (including the hardware, software and appropriate configuration). This procedure includes a build checklist, server hardening checklist and pre-production testing. Baseline configurations for servers, network devices, and databases are consistent with industry-accepted CIS (Center for Internet Security) system hardening guidelines that address known security vulnerabilities. Prior to go-live with new infrastructure, management approval is required and the decision is based upon the results of the pre-production testing.
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	Pre-packaging development and quality environments for the MobileCaddy Application are segregated from the primary packaging environments via Salesforce instance separation. Access to each staged packaging environment follows the Segregation of Duties Policy. Development and/or quality environments for the Salesforce Services that host and run the MobileCaddy managed package are physically and logically segregated from production environments. Administrative access to these environments follows the Segregation of Duties Policy.
Infrastructure & Virtualization Security *Segmentation*	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance	The MobileCaddy managed package is hosted and runs on Salesforce's multitenant architecture and secure logical controls for the Salesforce Services address the separation of Customer Data. Salesforce does not use dedicated servers used for a specific customer. The infrastructure for the Salesforce Services is divided into a modular architecture based on instance. Each instance is capable of supporting several thousand customers in a secure and efficient manner.

Control Area	Control ID	Control Specification	Control Notes
		- Compliance with legal, statutory, and regulatory compliance obligations	
Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Not applicable. The Salesforce Services that host and run the MobileCaddy managed package do not utilize virtualization in the provision of the Salesforce Services.
Infrastructure & Virtualization Security *Hypervisor Hardening*	IVS-11	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Not applicable. The Salesforce Services that host and run the MobileCaddy managed package do not utilize virtualization in the provision of the Salesforce Services.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: - Perimeter firewalls implemented and configured to restrict unauthorized traffic - Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) - User access to wireless network devices restricted to authorized personnel	The MobileCaddy managed package is hosted and run on Salesforce Services and infrastructure. Salesforce system and network configuration (including the use of perimeter firewalls), use of encryption, and rogue wireless detection for the Salesforce Services are required by Salesforce's internal policies and standards and are audited regularly against applicable compliance frameworks.

Control Area	Control ID	Control Specification	Control Notes
		- The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	The MobileCaddy managed package is hosted and run on Salesforce Services and infrastructure. Salesforce implements a multi-tiered network architecture for the Salesforce Services. Multilevel security products from security vendors and security practices help ensure network security. To help prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches help ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors help protect all network segments. Salesforce internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.
Interperability & Portability *APIs*	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	There are a number of integration points on the Force.com platform, which is part of the Salesforce Services and where the MobileCaddy managed package application is hosted and runs. From a developer perspective, customers can invoke web services from the platform, or expose classes on the platform as web service endpoints. Customers can also interact with external HTTP endpoints, react to incoming email messages, and have automated outbound messages sent when certain events occur. Customers can use the Force.com Web Services API. There is a SOAP-based web services API, as well as a REST-based web services API, that provide direct access to data within a customer's organization. Using these APIs, client can be created to integrate with Force.com from a customer's language of choice. Toolkits that wrap around this API provide utility classes that make this integration even easier for a range of languages, including Java, .NET, PHP, Objective C, Ruby and Adobe Flex. View additional details on this topic here: http://bit.ly/SalesforceAPI

Control Area	Control ID	Control Specification	Control Notes
			The MobileCaddy Container Applications utilise Saleforce Javascript Remoting via an AJAX request from a Visualforce page directly to an Apex controller. JavaScript remoting allows you to run asynchronous actions by decoupling the page from the controller and to perform tasks on the page without having to reload the entire page.
Interperability & Portability *Data Request*	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Several methods exist to export data from the Salesforce Services where the MobileCaddy managed package is hosted and runs. This allows Customer Data including configuration data for the MobileCaddy managed package to be exported. • Direct Export - Data can be exported directly into CSV (comma separated values) file, or Excel files with a button click. This can be done from either a standard or custom list view, or from a report. This is the most common method utilized by end users. • Excel Connector - Salesforce provide an Excel Connector to push and pull data from Excel to Salesforce Services and vice Versa. • Salesforce API - Data can be exported to and from the system though Salesforce's API at any time or via a number of built in Features. • Salesforce Data Loader - The Salesforce Apex Data Loader is a free tool which is used specifically for importing/updating/exporting data in Salesforce Services. The Salesforce Services also offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system). Unstructured data is provided in the same file format as the original data, e.g. .jpg, .pdf, .docx.

Control Area	Control ID	Control Specification	Control Notes
Interperability & Portability *Policy & Legal*	IPY-03	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	The Force.com platform which is part of the Salesforce Services where the MobileCaddy managed package is hosted and runs provides open, standards-based APIs that developers can use to build apps. Both RESTful and Web services (SOAPbased) APIs are available that provide access to Force.com's many features. Salesforce maintains a Developerforce site with details of the APIs supported and Developers guides for the various APIs. Refer here for information on Integration options: http://wiki.developerforce.com/page/Integration Refer here for Developer Guides under the Integration heading: http://wiki.developerforce.com/page/Documentation
Interperability & Portability *Standardized Network Protocols*	IPY-04	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Please refer to the responses provided to IVS-06, IPY-01, IPY-02, and IPY-03 above.
Interperability & Portability *Standardized Network Protocols*	IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	Not applicable. The Salesforce Services that host and run the MobileCaddy managed package do not utilize virtualization in the provision of the Salesforce Services.

Control Area	Control ID	Control Specification	Control Notes
Mobile Security *Anti-Malware*	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who manage and host Customer Data and the MobileCaddy managed package provides security awareness training to its employees covering topics such as working remotely, information security policies (which have sections dedicated to acceptable use and mobile security), and mobile devices, including discussion of authorized devices, laptop security, and social media.
Mobile Security *Application Stores*	MOS-02	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Acceptable use of mobile devices and appropriate locations for storage of Customer Data is addressed in Salesforce's Information Security policies applicable to the Salesforce Services. Customer Data is not stored by Salesforce on portable or mobile devices and technical controls are in place to prevent the transfer of Customer Data to portable media by Salesforce users with logical access to manage the Salesforce Services' production Systems. Customers control data storage configuration on mobile devices for their users. If data is cached or stored on mobile devices, the data is encrypted on the device. When utilising the MobileCaddy managed package Customers can further control access by their users and the data available to their users via MobileCaddy configuration settings.
Mobile Security *Approved Applications*	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce Services which host the MobileCaddy manage package is covered by Salesforce's Information Security policies address the installation of only approved applications and the prohibition of installing unapproved applications on mobile devices. MDM (Mobile Device Management) tools control the installation and use of approved applications.

Control Area	Control ID	Control Specification	Control Notes
Mobile Security *Approved Software for BYOD*	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce Services which host the MobileCaddy manage package is covered by acceptable use of BYOD devices under Salesforce's Information Security policies and security awareness training. As previously noted, Customer Data is not stored by Salesforce on portable or mobile devices and technical controls are in place to prevent the transfer of Customer Data to portable media by Salesforce users with logical access to manage the production systems.
Mobile Security *Awareness and Training*	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce which hosts and runs the MobileCaddy managed package and Customer Data has a documented mobile device security policy as part of the Salesforce's information security policies. Please also refer to the prior Mobile Security responses above.
Mobile Security *Cloud Based Services*	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Please refer to the prior Mobile Security responses provided above.
Mobile Security *Compatability*	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. For Salesforce who provide the hosting the MobileCaddy managed package application and Customer Data new mobile devices or different operating system versions being allowed for connection to Salesforce's corporate assets, they must be tested and validated by both Salesforce corporate IT and Trust (Information Security).
Mobile Security *Device Eligibility*	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Please refer to the prior Mobile Security and BYOD responses provided above.

Control Area	Control ID	Control Specification	Control Notes
Mobile Security *Device Inventory*	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who provide the hosting for the MobileCaddy managed package and Customer Data uses a Mobile Device Management (MDM) solution to manage the distribution of applications, data and configuration settings for mobile devices allowed in the Company's corporate environment. Through the use of MDM technologies, Salesforce maintains an inventory of devices allowed to store and access corporate data. As previously noted, Customer Data is not stored by Salesforce on mobile devices.
Mobile Security *Device Management*	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Please refer to the response provided to MOS-09 Device Inventory above.
Mobile Security *Encryption*	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and shall be enforced through technology controls.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who provide the hosting for the MobileCaddy managed package application and the Customer Data ensure the capability for encryption of data on mobile devices is included in the evaluation and validation of new mobiles devices allowed in the environment and described in response to MOS-07 Compatibility provided above.
Mobile Security *Jailbreaking and Rooting*	MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who provide the hosting for the MobileCaddy managed package application and the Customer Data prohibit Jailbreaking and Rooting by the Salesforce mobile device policy. Please also refer to the details around use of MDM technology in response to MOS-07 Compatibility provided above.

Control Area	Control ID	Control Specification	Control Notes
Mobile Security *Legal*	MOS-13	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case that a wipe of the device is required.	Please refer to the prior Mobile Security responses above. The Salesforce Services which host the MobileCaddy managed package and the customer data, addresses the potential for monitoring of activity on BYOD devices with access to corporate data, potential requirements for e-discovery or legal holds, and the potential loss of non-company data in the event a wipe of a BYOD device is required via Salesforce mobile security policy.
Mobile Security *Lockout Screen*	MOS-14	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who provide the hosting for the MobileCaddy managed package application and the Customer Data addresses automatic password lockout requirements, including, minimum character length, and passlock expiration via the Salesforce mobile security policy . The Password format is defined and administered by Salesforce Corporate IT.
Mobile Security *Operating Systems*	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who provide the hosting for the MobileCaddy managed package application and the Customer Data addresses changes to mobile device operating systems, patch levels, and/or applications are managed via MDM. Please refer to the responses provided to MOS-09 Device Inventory and MOS-07 Compatibility above.
Mobile Security *Passwords*	MOS-16	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who provide the hosting for the MobileCaddy managed package application and the Customer Data addresses password policies and password usage for Salesforce personnel using mobile devices by the mobile security policy, and are enforced by MDM. Please refer to the responses provided to MOS-09 and MOS-14 above.

Control Area	Control ID	Control Specification	Control Notes
Mobile Security *Policy*	MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce who provide the hosting for the MobileCaddy managed package application and the Customer Data addresses malware concerns for mobile devices and data backups used by Salesforce personnel via the Salesforce mobile device policy . The policy prohibits the transmission or storage of Salesforce company and customer information on external devices and systems not procured by the company.
Mobile Security *Remote Wipe*	MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce, who provide the hosting for the MobileCaddy managed package application and the Customer Data, through the use of MDM, Salesforce may remote wipe its employees' mobile devices. Employees must agree to download the MDM client to corporate-owned or BYOD devices in order to access corporate systems and assets.
Mobile Security *Security Patches*	MOS-19	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce, who provide the hosting for the MobileCaddy managed package application and the Customer Data, require their employees to download the latest security patches for mobile devices that have been approved by Corporate IT and Trust. This is managed via MDM. Please refer to the response provided to MOS-07 Compatibility above.
Mobile Security *Users*	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	The MobileCaddy managed package is hosted and runs on Salesforce Services. MobileCaddy employees have no access to Customer Data generally and specifically on Mobile Devices. Salesforce, who provide the hosting for the MobileCaddy managed package application and the Customer Data, addresses what systems and servers are allowed for use or access on a mobile device by Salesforce employees via the Salesforce mobile security policy.

Control Area	Control ID	Control Specification	Control Notes
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	The MobileCaddy managed package is hosted and runs on Salesforce Services along with all Customer Data. Salesforce liaises with external counsel, security and privacy organizations, and industry associations where appropriate to help ensure security and privacy compliance. Salesforce maintains contacts with law enforcement authorities, including local and federal authorities. Updates to requirements are made to the MobileCaddy managed package through updates to the Salesforce ISV certification and recertification process.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Salesforce has a formal Incident Management Process applicable to the Salesforce Services that host the MobileCaddy managed package along with Customer Data. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an internal ticketing system.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	The MobileCaddy managed package is hosted and runs on Salesforce Services along with all Customer Data. No MobileCaddy employees have access to the Customer Data or Salesforce Services subscribed to by the Customer. To the extent that MobileCaddy employees may be aware of potential or actual Salesforce security breaches they are trained and updated via regular meetings that if they know or suspect a breach to contact the Salesforce security team. Salesforce employees are informed through regular information security trainings that if they know or suspect there is a breach of security, it must be reported to the individual's manager or Information Security. Salesforce new hire orientation includes the Salesforce Code of Conduct, which states that Salesforce employees must safeguard Customer Data and report violations of the Code, under consequences of termination of employment and civil and legal action. The new hire process also includes signing a receipt for the Employee Handbook, the Code of Conduct, and signing a confidentiality agreement. Third party suppliers that support the Salesforce Services, with potential access to Customer Data, are contractually required to notify Salesforce of information security events involving Customer Data.

Control Area	Control ID	Control Specification	Control Notes
			Salesforce will promptly notify the Customer in the event of any security breach of the Service resulting in an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce Support, email to customer's administrator and Security Contact (if submitted by customer).
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	The MobileCaddy managed package is hosted and runs on Salesforce Services along with all Customer Data. No MobileCaddy employees have access to the Customer Data or Salesforce Services subscribed to by the Customer. In the event of a security incident, proper forensic procedures including chain of custody will be performed for collection, retention, and presentation of evidence by Salesforce. In the event of an actual or reasonably suspected unauthorized disclosure of Customer Data, Salesforce will inform affected customers of the details of the incident to the extent legally permissible and any actions being taken to remediate and prevent further breaches from occurring.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Salesforce host and run the MobileCaddy managed package and Customer Data. The Salesforce CSIRT follows an Incident Response plan, which includes the process for monitoring reports and alerts and responding to security incidents. Incident analysis includes data for response process improvement on an ongoing basis.
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Third parties engaged in the provision of the Salesforce Services which hosts and runs the MobileCaddy managed package are required to enter into contracts with Salesforce including confidentiality provisions, background screening requirements, training and breach of policy and enforcement provisions.

Control Area	Control ID	Control Specification	Control Notes
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Salesforce who host and run the MobileCaddy managed package and Customer Data has a formal Incident Management Process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an Salesforce internal ticketing system. Please refer to the response provided to SEF-03 Timely Reporting of Security Events above.
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Salesforce host and run the MobileCaddy managed package and Customer Data and contracts with its colocation facilities and network service providers for the Salesforce Services include provisions for capacity, resiliency, and service delivery. Please also refer to the responses provided to BCR-01, BCR-03, BCR-09 and IVS-04 above.
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	Please refer to the response provided to STA-01 Data Quality and Integrity above.
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-05	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced	The MobileCaddy managed package is hosted and run by Salesforce Services. Customer Contracts with Salesforce' include many of the topics described. Please refer to the standard Salesforce Services Master Subscription Agreement (MSA) for details: http://www2.sfdcstatic.com/assets/pdf/misc/salesforce_MSA.pdf Salesforce Services Documentation describing the Security and Compliance practices: https://help.salesforce.com/apex/HTViewSolution?urlname=Salesforce-Services-Trust-and-Compliance-Documentation&language=en_US

Control Area	Control ID	Control Specification	Control Notes
		business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	Also Refer to the MobileCaddy Master Subscription Agreement (MSA) for details: http://www.mobilecaddy.net/mobilecaddy-end-user-services-agreement/

Control Area	Control ID	Control Specification	Control Notes
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Please refer to the response provided to STA-01 Data Quality and Integrity above.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Please refer to the response provided to STA-01 Data Quality and Integrity above.
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.	Please refer to the response provided to STA-01 Data Quality and Integrity above.
Threat and Vulnerability Management *Anti-Virus / Malicious Software*	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile	The MobileCaddy managed package is hosted and run by Salesforce Services. Customer Data is not stored by Salesforce on Salesforce endpoint devices. The production environment for the Salesforce Services is managed via a secure remote client that prevents the ability for malware to traverse from the local client laptop or desktop to the hosted environment. Salesforce has anti-virus programs installed on systems which support the Salesforce Services. Salesforce runs anti-virus software on the production systems, which are Linux or Unix based.

Control Area	Control ID	Control Specification	Control Notes
		devices) and IT infrastructure network and systems components.	Other controls are also used to address malware such as hardening the operating system of servers, firewall configuration to ensure only required ports are open and all others denied, and implementing intrusion detection systems. Access to these systems is restricted to authorized personnel and all these systems, as well as the host platforms, are monitored in real-time through a security event monitoring system.
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Salesforce regularly performs self-vulnerability assessments for the Salesforce Services which host and runs the MobileCaddy managed package and the Customer Data, using various tools and techniques, including network-layer vulnerability scans, application-layer vulnerability scans, and local operating system-layer vulnerability scans. Depending on the severity and the risk to Salesforce systems, security patches can be scheduled for immediate deployment or deferred to an appropriate planned maintenance interval.
Threat and Vulnerability Management *Mobile Code*	TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Salesforce has controls over mobile code within its corporate environment. Customers have the ability to utilise mobile code and it is their responsibility to secure end-systems and implement a security policy in regards to appropriate use of mobile code. When utilising the MobileCaddy managed package and the MobileCaddy Container Applications the Customer Data retrieved, queried and stored maintains the Customers data visibility and security models as defined by the Customers System Administrators with Salesforce features such as Organisation Wide Sharing settings, employee roles and Salesforce User Profiles. The MobileCaddy package and Container Applications are certified through a regular (at least annual) Security Review to ensure code executed and records retrieved comply with the Salesforce security and sharing features that the Customer configures.