

DIRECTV Supplier Information Security Requirements (SISR) v4.0 September 2026

1.0 Introduction

1.1 Applicability

The following DIRECTV Supplier Information Security Requirements ("Security Requirements") apply to Supplier Entities' Information Resources used when performing any action, activity, or work under this Agreement where any of the following occur (hereinafter referred to as "In-Scope Work"):

1. The collection, processing, storage, handling, backup, disposal, and/or access to In-Scope Information;
2. Providing or supporting DIRECTV-branded applications and/or services using non-DIRECTV Information Resources;
3. Access to DIRECTV's Information Resources;
4. The development or customization, outside of mere configuration changes, of any software for DIRECTV; or
5. Website hosting and/or development for DIRECTV.

These Security Requirements do not (i) apply to commercial off the shelf products or materials acquired from a Supplier Entity unless Supplier performs In-Scope Work, or (ii) limit more stringent obligations, if any, such as privacy or security patching as set forth elsewhere in the Agreement.

1.2 Evidence of Compliance

- 1.2.1 Supplier must provide DIRECTV or its delegate, in a timely manner as reasonably requested by DIRECTV:
 - a. Evidence of compliance with these Security Requirements, which includes copies of policies, procedures, reports, and other documentation supporting such compliance; and
 - b. A high-level network data flow diagram depicting cloud/non-cloud Information Resources and encrypted/non-encrypted data flows where In-Scope Information is in transit or at rest.
 - c. Current evidence of Cybersecurity Insurance Certificate as required in the Agreement.

2.0 Security Domain

Supplier Entity must:

2.1 Corporate Policy Compliance

- 2.1.1 Implement, maintain, and adhere to documented Cybersecurity and Cybersecurity awareness program(s).
- 2.1.2 Implement, maintain, and adhere to documented policies for:
 - a. Any business continuity plan and/or disaster recovery plan requirements under the Agreement;
 - b. Any retention, return, and/or destruction requirements for In-Scope Information under the Agreement; and
 - c. Ensuring that In-Scope Information is only used for the performance of In-Scope Work.

2.2 Asset Management Security

- 2.2.1 Harden Information Resources used to perform In-Scope Work by:
 - a. using a minimum-security baseline configuration based upon industry best practices to reduce potential ways of attack, including limiting software and services to only those required and;
 - b. Changing default passwords, prohibiting weak passwords and exact matches to the UserID, removing unnecessary software, UserIDs, usernames, or logins, and disabling or removing unnecessary services (this requirement is not intended to apply to software that is part of a standard software configuration). Such hardening is to prevent exploits that attack flaws in the underlying code and must be applied to Information Resources in Supplier Entities' networks, as well as those networks hosted by Cloud Service Providers; and
 - c. Not using Information Resources to perform In-Scope Work past the date when:
 - i. They will no longer be supported by issued security updates which include whenever a Supplier Entity ceases to obtain and/or implement such security updates (for example, if a Supplier Entity ceases to purchase and/or extend the maintenance services under which such security updates are provided); or
 - ii. Any extended security patching support ends.
- 2.2.2 Implement, maintain, and adhere to documented policies to:
 - a. Install and run a current industry-standard antivirus solution to scan for and promptly remove or quarantine viruses and other malware; and
 - b. Configure end user devices to ensure end users are restricted from the ability to install unauthorized software or to disable required software.

- 2.2.3 Implement, maintain, and use documented policies, standards, and procedures for Portable Devices and laptop computers used to access and/or store In-Scope Information that include the following requirements:
- a. All users must be authorized for such access and their identity authenticated;
 - b. Portable Devices and laptop computers must be physically secured and/or in the physical possession of authorized individuals;
 - c. Where technically feasible, use a remote wipe capability on Portable Devices to delete promptly and securely In-Scope Information when such devices are not in the physical possession of authorized individuals or otherwise physically secured; and
 - d. Jailbroken or rooted Portable Devices cannot be used to perform In-Scope Work.
- 2.2.4 Implement, maintain, and use a documented policy that prohibits the use of any:
- a. Supplier Entity-issued Portable Devices and laptop computers to access and/or store In-Scope Information unless the device is administered and/or managed by a Supplier Entity; and
 - b. Non-Supplier Entity-issued Portable Devices and laptop computers to access and/or store In-Scope Information unless the device is segregated and protected by using a Supplier Entity-administered and/or -managed secure container-based and/or sandbox solution.

2.3 Data Protection

- 2.3.1 Use Strong Encryption when storing In-Scope Information:
- a. On all computing devices located in areas accessible by the public and physically secure such devices;
 - b. On Portable Devices and laptop computers, must have full disk encryption;
 - c. Within Cloud Service, including backups, archives, and logs; and
 - d. That is classified as DIRECTV's SPI or DIRECTV's SCD in all other environments.
- 2.3.2 Use Strong Encryption when transmitting or remotely accessing In-Scope Information:
- a. Via any network that is not controlled by DIRECTV or Supplier Entities, regardless of the technology;
 - b. Via all networks to, from, and within a Cloud Service;
 - c. Using radio frequency (RF) based wireless networking technologies (e.g., Bluetooth and Wi-Fi) except for the use of RF-based wireless headsets, keyboards, microphones, and pointing devices, such as mice, touch pads, and digital drawing tablets; and
 - d. Using secure protocols only (e.g. TLS,HTTPS, SSH, SFTP): clear-text protocols are prohibited; and

- e. That is classified as DIRECTV's SPI or SCD, regardless of the technology, over all other networks, including Supplier Entity networks.

2.3.3 Use proven, industry-standard cryptography and documented key management, and:

- a. Use algorithms accepted by recognized industry standard bodies (e.g., FIPS 140-3), such as AES, RSA/ECC, SHA-256/512/3, and HMAC; deprecated algorithms are prohibited;
- b. Protect keys against loss, modification, unauthorized use, and disclosure, and store and transmit keys separately from the data they protect;
- c. Restrict key access using least privilege, split knowledge, and dual control, and use separate keys for encryption and signing;
- d. Expire and replace keys upon certificate renewal or replacement, and at minimum every two (2) years;
- e. Renew certificates before expiration using trusted Certificate Authorities; and
- f. Securely destroy keys at end of lifecycle or contract.

2.3.4 Implement, maintain, and adhere to documented policies and controls for data loss prevention by ensuring that In-Scope Information is not exfiltrated.

2.4 Identity and Access Management

2.4.1 Use Identity and access management that includes:

- a. Enforcement of the rule of least privilege by requiring application, database, network, and system administrators to restrict access of all users to only the commands, In-Scope Information, and Information Resources necessary for them to perform authorized functions.
- b. Controls that are in place to limit, protect, monitor, detect and respond to all Administrative User activities. Controls that must be enforced include separation of duties, Individual accountability, authorization and approval.
- c. Integration or federation with a DIRECTV-approved identity access management solution, when providing access to a DIRECTV user, or a DIRECTV customer or mechanized account.
- d. Maintaining logs of identification, authentication, and authorization activities, and making such logs available to DIRECTV upon request.

- 2.4.2 Restrict access to security logs to authorized individuals and protect security logs from unauthorized modification.
- 2.4.3 Assign unique UserIDs to authorized Individual users, Administrative Users, and Service Accounts. Assign individual ownership to Service Accounts and maintain individual accountability at all times.
- 2.4.4 Maintain a documented UserID lifecycle change management policy for all Information Resources across all environments that includes:
 - a. Manual and/or automated processes for approved account creation and/or modification;
 - b. Account disabling upon user termination or the occurrence of any other condition rendering the account as no longer needed, followed by removal of the account within ninety (90) days;
 - c. Disabling and/or removing inactive accounts assigned to individuals after no more than forty five (45) days of inactivity except in cases where the account is assigned to a customer of DIRECTV or used by a current or retired employee of DIRECTV to process their own information; and
 - d. Initiating processes to review, no less than annually, access privileges and account validity for all users including Administrative Users.
- 2.4.5 Terminate interactive sessions on an end user's device, or activate a secure, locking screensaver requiring authentication, after a period of inactivity not to exceed fifteen (15) minutes. On all other Information Resources terminate inactive interactive sessions after a period not to exceed thirty (30) minutes.
- 2.4.6 Use Strong Encryption and/or one-way hashing based upon Strong Cryptography whenever authentication credentials are stored. This requirement applies to all classifications of users.
- 2.4.7 Implement, maintain and adhere to a policy to ensure password and authentication credentials must:
 - a. Not be shared;
 - b. Be complex and meet the following password construction requirements:
 - i. Be a minimum of eight (8) characters in length;
 - ii. Include characters from at least two (2) of these groupings: alpha, numeric, and special characters;
 - iii. Not to be the same as the UserID with which they are associated; and
 - iv. Expire at regular intervals not to exceed ninety (90) calendar days with the exception of Service Accounts which must expire at least annually.
 - c. Require a password reset at first login whenever a temporary credential is used or after a security incident has been detected. When providing a user with a new or

- reset password, or other authentication credentials, use a secure method to provide this information; and
 - d. Not be embedded (e.g., hardcoded passwords and SSH keys).
- 2.4.8 Require and enforce Multi-Factor Authentication (MFA):
- a. For any remote access use of Information Resources;
 - b. For all Administrative Users of Cloud Services; and
 - c. For administrative and/or management access to Security Gateways, including any access for the purpose of reviewing log files.
- 2.4.9 Notify Supplier's DIRECTV contact within one (1) business day when a Supplier Entity employee's authorized access to DIRECTV's Information Resources is no longer needed or must be modified.
- 2.4.11 For SaaS providers:
- a. Authenticate all identities used by DIRECTV users with DIRECTV-approved identity management solutions (e.g., SAML); and
 - b. Provide or make available to DIRECTV, access and/or authorization logs upon request.

2.5 Network Connectivity

- 2.5.1 Install and use Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) that monitor all traffic entering and leaving Information Resources in connection with In-Scope Work. Both Network and Host IDS/IPS are acceptable solutions. At a Supplier Entity's discretion, this requirement is optional for implementations of Host Intrusion Detection Systems (HIDS) and/or Host Intrusion Prevention Systems (HIPS) on mobile devices.
- 2.5.2 Ensure that Supplier Entities' Information Resources, when providing Internet-accessible services to DIRECTV, have Denial of Service (DoS/DDoS) and Security Gateway protections in place. Web servers must reside in a DMZ and Information Resources persistently storing In-Scope Information (such as application and database servers) must reside in an internal network.
- 2.5.3 Ensure that each Security Gateway rule is:
 - a. Properly authorized prior to implementation and is traceable to a specific business request; and
 - b. Explicitly or implicitly ends with a "DENY ALL" statement for each set and;
 - c. Reviewed annually for validity.

- 2.5.4 In the event that a Supplier Entity has or will be provided, access to DIRECTV's or DIRECTV's customers' Information Resources in connection with In-Scope Work, then the Supplier Entity must not establish additional interconnections to DIRECTV's and DIRECTV's customers' Information Resources without the prior consent of DIRECTV and must:
- a. Use only the mutually agreed-upon facilities and connection methodologies to interconnect DIRECTV's and DIRECTV's customers' Information Resources with Supplier's Information Resources;
 - b. Limit access of DIRECTV's and DIRECTV's customers' Information Resources to only Supplier Entity personnel who are designated and authorized to perform In-Scope Work; and
 - c. Disclose the intended use of and, upon DIRECTV's request, allow DIRECTV or its delegate to scan portable external storage devices (e.g., USB drive) prior to physically attaching them to Information Resources used for In-Scope Work.
- 2.5.5 Internet-facing applications using Hypertext Transfer Protocol (HTTP) or the Hypertext Transfer Protocol Secure (HTTPS) must implement security controls that filter and monitor application layer traffic, including customizable rules to detect and respond to application-specific threats, and managed rules that protect against current threats and vulnerabilities (e.g. OWASP Top 10).

2.6 Supplier Entity Security Compliance

- 2.6.1 For all Supplier Entities performing In-Scope Work, Supplier must:
- a. Ensure compliance with these Security Requirements, or requirements that are no less stringent;
 - b. Implement, maintain, and adhere to a documented program by which compliance to these Security Requirements is evaluated and all corrective actions are documented and implemented within no more than ninety (90) days; and
 - c. Provide documentation and/or evidence to substantiate such compliance, upon request.
 - d. In the event a Supplier Entity discovers they are not compliant, or DIRECTV finds a Supplier Entity to be non-compliant with these Security Requirements, Supplier Entity must cooperate with DIRECTV to document and promptly implement corrective action, but within no more than ninety (90) days after the Supplier Entity's initial discovery or DIRECTV's initial notification to the Supplier.

2.7 Information Resource Lifecycle

- 2.7.1 Segregate In-Scope Information from any other customer's and Supplier Entities' own information, either by using logical access controls and/or physical access controls to provide protection from unauthorized access.
- 2.7.2 Separate non-production Information Resources from production Information Resources and separate In-Scope Information from non-production Information Resources.
- 2.7.3 DIRECTV explicitly prohibits the use of In-Scope Information within any Artificial Intelligence (AI) platform or tool unless specifically authorized by DIRECTV in the agreement.
- 2.7.4 Maintain a documented change control policy including back-out procedures for all production environments.

2.8 Security Information and Event Management

- 2.8.1 Implement, maintain and adhere to documented policies and controls to:
 - a. Detect and terminate unauthorized attempts to access and/or change In-Scope Information, and/or system or application configuration files;
 - b. Log all successful and unsuccessful login attempts;
 - c. Log all logouts;
 - d. Log all successful and failed attempts to export, transmit, and access In-Scope Information.
 - e. Monitor and investigate unauthorized activity and remediate any successful unauthorized activity;
 - f. Maintain logs of all sessions accessing DIRECTV's Information Resources, if the agreed-upon connectivity methodology requires that Supplier Entity implement a Security Gateway. Such session logs must include origination IP address, destination IP address, ports/service protocols used, durations of access, and sufficiently detailed information to support a security incident or a forensic investigation (e.g., identification of the end user or application accessing DIRECTV); and
 - g. For any remote access use of Information Resources, continually log, detect, and:
 - i. Terminate unauthorized remote access attempts (e.g., geolocation restrictions, anonymous VPN, and known bad actors); and
 - ii. Investigate for potential termination of connections to any Supplier Entity user or system performing In-Scope Work from countries other than those specifically allowed under the Agreement.

- 2.8.2 For applications which use a database that allows modifications to In-Scope Information, create logs:
- By enabling database transaction logging features where transaction logging is supported; or
 - By implementing another mechanism that logs all modifications to In-Scope Information stored within the database, including timestamp, UserID, and information modified, where transaction logging is not supported.
- 2.8.3 Review, on no less than a weekly basis, Administrative User activities and all anomalies from security and security-related audit logs and document and resolve logged security problems in a timely manner. Automated processes may promptly issue alarms and/or alerts that cause prompt investigation and review by responsible individuals and, if automated processes successfully resolve a logged security problem, no further action by responsible individuals is required.
- 2.8.4 Retain all logs for a minimum of three (3) months (or thirteen (13) months if required by Sarbanes-Oxley Act (SOX), Payment Card Industry (PCI), and GDPR related security audit logs) either on-line or on backup media.
- 2.8.5 For threats, vulnerabilities, and non-compliances:
- When presented with evidence by DIRECTV of a threat to DIRECTV's or DIRECTV's customers' Information Resources originating from the Supplier Entities' networks (e.g., worm, virus or other malware, bot infection, Advanced Persistent Threat (APT), DoS/DDoS attack, etc.), promptly cooperate and cause any other Supplier Entities to promptly cooperate with DIRECTV and take all reasonable and necessary steps to isolate, mitigate, terminate, and/or remediate all known or suspected threats;
 - When a Supplier Entity learns of or discovers a known threat/vulnerability impacting DIRECTV or DIRECTV's customers (including notifications received from security researchers, industry resources, or Ethical Hacking and Responsible Disclose Program promptly notify and cooperate with DIRECTV, and take all reasonable and necessary steps to isolate, mitigate, and/or remediate such known threat/vulnerability; and
 - In the event a Supplier Entity discovers that it is non-compliant, or DIRECTV finds a Supplier Entity to be non-compliant with these Security Requirements, implement corrective action promptly, but within no more than ninety (90) days after the Supplier Entity's initial discovery or DIRECTV's initial notification to the Supplier.
 - When persistent findings through DIRECTV's Bug Bounty Program or Ethical Hacking and Responsible Disclose Program, may trigger further review, corrective actions, and potential cost recovery. Supplier Entities will be notified in writing, with relevant evidence, prior to the enforcement of any reimbursement requirements.
- 2.8.6 Contact details of Supplier's designated security personnel must be provided upon request. This information must include, but is not limited to, the name, title, email address, and phone number of the primary and secondary security contacts. Suppliers

must ensure that these contacts are available and responsive to address any security-related inquiries or incidents in a timely manner. Supplier must email DIRECTV's Business Contact with written notice of any changes to such contacts within one (1) calendar day, and such changes and notice will not require an amendment to this Agreement.

- 2.8.7. Maintain a documented procedure that must be followed in the event of a suspected attack upon, intrusion upon, unauthorized access to, loss, including theft of, or other security breach involving In-Scope Information and/or Supplier Entity-owned, -managed, or -used Portable Devices and/or laptop computers containing In-Scope Information in which Supplier must promptly:
- a. Investigate or cause Supplier Entities to investigate to determine if such an attack has occurred; and
 - b. Notify DIRECTV if a confirmed attack including unauthorized access of In-Scope Information has occurred by contacting DIRECTV Helpdesk by telephone at:
 - i. 1-855-485-6979 from within the US, or
 - ii. 1-855-652-1516 from Puerto Rico, or
 - iii. 1-844-419-2818 from Canada or
 - iv. by email at helpdesk@mydirectv.com.
 - v. And Supplier's DIRECTV Business Unit contact.

2.8.8 Provide DIRECTV with:

- a. Regular status updates whenever there is a confirmed attack upon, intrusion upon, unauthorized access to, loss of, including theft of, or other breach of In-Scope Information and/or Supplier Entity-owned, -managed or -used Portable Devices and/or laptop computers containing In-Scope Information. These status updates must include the actions taken to resolve the incident and must be provided at mutually agreed upon intervals for the duration of the incident.
- b. Within seven (7) calendar days of the closure of the incident, provide DIRECTV with a written report describing the incident, actions taken by the Supplier Entity during its response, and Supplier Entity's plans for future actions to prevent a similar incident from occurring.

2.9 Vulnerability Management

- 2.9.1 Implement, maintain, and adhere to a documented vulnerability management policy for all Information Resources to:
- a. Monitor industry resources (e.g., www.cert.org, the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), pertinent software vendor mailing lists and websites, and information from subscriptions to automated notifications) for timely notification and current statuses of all applicable security alerts and vulnerability reports that pertain to Information Resources;
 - b. Perform at least quarterly, host-based or network-based scans.

- c. For all other software used to perform and/or support In-Scope Work, review and scan such software prior to initial deployment, upon code changes, and at least annually; and
- d. For all internet-accessible applications used to support In-Scope Work, perform penetration testing at least annually.

2.9.2 For all software developed or customized, outside of mere configuration changes, for DIRECTV and intended to run on DIRECTV's Information Resources under the Agreement:

- a. Implement, maintain, and adhere to a documented vulnerability management policy that includes:
 - i. Static Analysis Security Testing (SAST) including Software Composition analysis (SCA) must be performed prior to initial deployment, upon code changes, and at least every 6 months but quarterly for DIRECTV SPI, SOX, PCI, and internet-facing or mobile applications;
 - ii. Dynamic Analysis Security Testing (DAST) must be performed for all web applications prior to initial deployment, upon code changes, and at least every six (6) months but quarterly for DIRECTV SPI, SOX, PCI, and internet-facing or mobile applications;
 - iii. Penetration testing at least annually; and
 - iv. Upon request, make scan results and remediation plans available to DIRECTV.
- b. Apply appropriate security patches or otherwise render the vulnerability not exploitable for all security vulnerabilities with a risk or severity rating of critical, high, or medium identified on Supplier Entities' Information Resources, within the following risk-based timeframe:
 - i) Critical – within thirty (30) days, unless the risk requires an accelerated schedule.
 - ii) High – within sixty (60) days
 - iii) Medium – within ninety (90) days

2.9.2 For all software developed or customized, outside of mere configuration changes, for DIRECTV and intended to run on DIRECTV's Information Resources, implement, maintain, and adhere to a documented vulnerability management policy that includes:

- a. Performing security scanning as follows (making results and remediation plans available to DIRECTV upon request):
 - i. Static Analysis Security Testing (SAST) including Software Composition Analysis (SCA) must be performed prior to initial deployment, upon code changes, and at least every six (6) months (quarterly for DIRECTV SPI, SOX, PCI, internet-facing and mobile applications);

- ii. Dynamic Analysis Security Testing (DAST) must be performed prior to initial deployment, upon code changes, and at least every six (6) months (quarterly for DIRECTV SPI, SOX, PCI, internet-facing and mobile applications);
 - iii. Penetration testing at least annually;
- b. Promptly provide a patch that renders the vulnerability non-exploitable upon discovery or notification of an exploitable vulnerability of software developed or customized, outside of mere configuration changes, for DIRECTV and installed on DIRECTV Information Resources, within the following risk-based timeframe:
 - i. Critical – within thirty (30) days, unless the risk requires an accelerated schedule.
 - ii. High – within sixty (60) days
 - iii. Medium – within ninety (90) days
 - iv. Low – within an agreed-upon timeframe

2.10 Payment Card Industry Data Security Standard Compliance:

To the extent that services and/or materials provided by, or on behalf of Supplier store, process, transmit cardholder data, or provide services which may impact the security of cardholder data, or the Cardholder Data Environment (CDE) Supplier must:

- a. Comply with the Payment Card Industry Data Security Standard (PCI DSS), at its own expense, for all systems, networks, and services in scope.
- b. Maintain PCI DSS compliance for the duration of the engagement and ensure compliance is aligned with the current version of the PCI DSS updated by the Payment Card Industry Security Standards Council, including any successor standard thereto applicable to the services provided.
- c. Upon request, provide a current Attestation of Compliance or Report on Compliance, as applicable and notification of any material changes affecting PCI DSS scope or compliance status.
- d. Ensure any subcontractor with access to cardholder data or systems impacting the CDE is PCI DSS compliant and maintain written agreements with such subcontractors that include PCI DSS obligations consistent with these requirements. The Supplier acknowledges and agrees that it is responsible for the security of cardholder data within its custody or control, including any subcontractors or third parties engaged by the Supplier.
- e. Notify DIRECTV without undue delay upon discovery of any actual or suspected security incident involving cardholder data and cooperate fully with incident response, forensic investigations, and regulatory or card brand reporting requirements. The Supplier shall promptly take all reasonable and appropriate actions to contain, investigate, mitigate, and remediate the incident in accordance with PCI DSS requirements and shall, upon request, permit reasonable validation of the PCI DSS compliance, including providing documentation and evidence necessary to support compliance verification for the services provided to DIRECTV.

Failure to maintain PCI DSS compliance or to meet the obligations outlined herein may result in remediation requirements, suspension of services, or termination of the agreement, at DIRECTV's discretion.

2.11. Physical Security

2.11.1 Ensure all Information Resources intended for use by multiple users and any areas where In-Scope Information is accessible are located in secure physical facilities with access restricted to authorized individuals only. For audit purposes, monitor and record access to such areas.

3.0 Definitions

Capitalized terms used within these Security Requirements but not defined herein shall have the meaning set forth in the Agreement.

“Administrative User” means a user with super user or elevated/enhanced security rights and permission for configuring, controlling, installing, or managing Information Resources, regardless of the types of devices and environments managed, including within any Supplier Entity’s facilities, such as within Cloud Service Provider (CSP) cloud environments.

“Business Unit Contact” means the DIRECTV employee that the Supplier works with on a regular basis and provides the contracted services.

“Cloud Service” means a service delivered via an “as a Service” cloud service model (e.g., Software as a Service (SaaS), Storage as a Service (STaaS), Database as a Service (DBaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)).

“Cloud Service Provider” or “CSP” means a Supplier Entity providing cloud-based computing services.

“Cybersecurity” means the protection of Information Resources and In-Scope Information from attacks, data theft, breaches, unauthorized access, social engineering, credential sharing, and other similar security threats.

“Demilitarized Zone” or “DMZ” means a physical or logical network or sub-network that separates an internal network from an outside network, such as the public Internet.

“In-Scope Information” means DIRECTV’s confidential and proprietary data, including DIRECTV Customer Information, which Supplier Entities collect, process, store, handle, or access in any manner while fulfilling their obligations under this Agreement, irrespective of the format and means of transmission.

“Information Resource(s)” means systems, applications, websites, networks, network elements, and other computing and information storage devices, along with the underlying technologies and delivery methods (e.g., social networks, mobile technologies, laptop computers, Portable Devices, Cloud Services, data analytics, call and voice/video recording, and Application Program Interfaces (APIs)).

“Multi-Factor Authentication” (also known as “MFA,” “Two-Factor Authentication,” and “Strong Authentication”) means the use of at least two of the following three types of authentication factors:

- A physical or logical credential the user has, such as an electronically readable badge, a token card, or a digital certificate;
- A knowledge-based credential, such as a password or PIN; and
- A biometric credential, such as a fingerprint or retina image.

“Portable Devices” means media and systems, with the exception of laptop computers, capable of being easily carried, moved, transported, or conveyed that are used in connection with In-Scope Work. Examples of such devices include tablets, USB hard drives, USB memory sticks, Personal Digital Assistants (PDAs), and mobile phones (e.g., smartphones).

“Security Gateway” means a set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers. Examples include firewalls, firewall management servers, hop boxes, session border controllers, proxy servers, and intrusion prevention devices.

“SCD” or “Sensitive Customer Data” means customer data that has been assessed as requiring a higher level of protection. SCD refers to the data elements listed in the [Table 2 - DIRECTV SCD Data Elements](#) located at the end of these Security Requirements. All data elements in Table 2 are considered In-Scope Information.

“SPI” or “Sensitive Personal Information” means private, personal information that, if compromised or exposed, could present a risk to individuals and would legally require DIRECTV to disclose the exposure. SPI refers to the data elements listed in the [Table 1 - DIRECTV SPI Data Elements](#) located at the end of these Security Requirements. All data elements in Table 1 are considered In-Scope Information.

“Service Account” means a UserID used for installing, executing, or administering an application or system. Service Accounts manage the local events/processes of an application or system.

“Strong Cryptography” means the use of cryptography based on industry-tested, accepted, and uncompromised algorithms and proper key management practices which incorporate a documented policy for the management of the encryption keys, and associated processes adequate to protect the confidentiality and privacy of the keys and credentials used as inputs to the cryptographic algorithm.

“Strong Encryption” means the use of encryption technologies based upon Strong Cryptography.

“Supplier Entity” or “Supplier Entities” means the Supplier, its affiliates, and their respective Subcontractors (including Cloud Service Providers).

4.0 Table 1 - DIRECTV SPI Data Elements

Data elements in the following tables must be treated as SPI when used in their entirety, unless explicitly stated otherwise. This applies to all data formats including scanned images, screen captures and recordings, PDFs, JPGs and any other unified communication, and collaboration tools/content.

4.1 Individual Identification and Familial Information

Data Element	Description
Government Issued Identification Number	Includes: 1. Driver’s License Number 2. Taxpayer Identification Number - In an individual’s name. Excludes those in a company name. 3. U.S. Social Security Number 4. National/State/Region issued identity number 5. Government Identity Card 6. Government identifiers for professionals 7. Government-sponsored health or food plan identifier 8. Passport Number 9. Alien Registration Number 10. Birth Certificate Number 11. Other government issued identification number Excludes: 1. Customer Application Identification Number (Application ID), and 2. Representative Accountability Database (RAD) ID, and

	3. Any such numbers that are issued on the understanding that they must be a matter of public record, e.g., U.S. FCC Radio License.
Date of Birth (DOB)	An individual's full and complete date of birth (DOB), i.e., including month, day, and year. Excludes partial DOB.

4.2 Financial Data

Data Element	Description
Payment Card Number	Primary Account Number (PAN) for all types of payment cards. Includes: 1. DIRECTV corporate payment card number 2. Consumer payment card number
Payment Card Security Data	The security data used in association with a payment card (corporate, personal, etc.) to confirm legitimate use. Includes: 1. Card Security Codes (CSC) 2. Personal Identification Numbers (PINs) used with payment cards but excludes PINs used to authenticate access to DIRECTV systems (see "Customer Authentication Credentials" data element).
Financial Institution Account Number	Includes: All types of financial institution accounts (savings, checking, investments, pensions, etc.) both personal and business in an individual's name. Excludes: Bank routing number.

4.3 Computer Identification and Authentication

Data Element	Description
Biometric Data	Measures of human physical and behavioral characteristics used for authentication purposes, for example DNA, fingerprint, voiceprint, retina, or iris image. Includes: Full biometric data. Excludes: 1. Templates (e.g., "vector" equivalents) that contain discrete data points derived from biometric data (i.e., templates that do not hold the complete biometric image, where the template cannot be reverse engineered back to the original biometric image), and genetic test information. 2. Signature.
Customer Authentication Credentials Applies to Customers only	Values used by customers to authenticate and permit access to:

	1. The customer’s personal information, including Customer Proprietary Network Information (CPNI) and DIRECTV Proprietary Information (SPI) — or — 2. An application enabling the customer to subscribe to, or unsubscribe from, DIRECTV services — or — 3. An DIRECTV service to which the customer is subscribed Includes: 1. Personal Identification Numbers (PINs), passwords, and passcodes 2. Templates (e.g., “vector” equivalents) of biometrics, photographs, or signatures Excludes: 1. Card Security Codes (CSCs) and PINs used in association with payment cards. 2. Full biometrics 3. Full photograph 4. Full signature
Customer Authentication Credential Hints Applies to Customers only	Answers to questions used to retrieve customer authentication credentials.
Work Vehicle Location	Information that identifies the current or past location of a DIRECTV work vehicle that is directly associated with a personal identifier for a DIRECTV Employee or Non-Payroll Worker (NPW) which allows for Location-Based Information tracking of such individual. The work vehicle’s location (e.g., a map address, or latitude and longitude together with altitude where known) may be determined because it is a connected vehicle or has some other Satellite Navigation (SatNav) capable device assigned to that vehicle, or by some other means such as network connectivity.
Location-Based Information (LBI)	Information that identifies the current or past location of a specific individual’s mobile device. A mobile device’s location (e.g., a map address, or latitude and longitude together with altitude where known) derived from the mobile device through activities such as GPS or network connectivity rather than as a result of user action (e.g., revealing location in the content of an email or SMS).

4.4 Background and Other Related Data

Data Element	Description
Criminal History	Information about an individual's criminal history, e.g., criminal check portion of a background check.
Background Checks	Third party (non-DIRECTV) checks, including credit history, employment history, and driving records. Excludes criminal history (see Criminal History).
Racial or Ethnic Origin Subject to non-U.S. Jurisdiction*	Data specifying and/or confirming an individual's racial or ethnic origin.
Trade Union Membership Subject to non-U.S. Jurisdiction*	Data specifying and/or confirming that an individual is a member of a trade union.
Information Related to an Individual's Political Affiliation or Religious Belief	Data specifying and/or confirming an individual's political affiliation or religious or similar beliefs.
Information Related to an Individual's Sexual Orientation Subject to non-U.S. Jurisdiction*	Data specifying and/or confirming an individual's sexual life or orientation.

4.5 Health Data

Data Element	Description
U.S. Protected Health Information (PHI)	Includes: - Any U.S. health information used in DIRECTV's Group Health Care plans or belonging to DIRECTV's customers that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individuals that includes information about: - The individual's past, present, or future physical or mental health or condition; - The provision of health care to the individual; — or — - The past, present, or future payment for the provision of health care to the individual. - Health information of retirees, employees, or employee beneficiaries used by DIRECTV for purposes other than a group health plan is not PHI. For medical and health information not related to DIRECTV's Group Health Care plans, see "Medical and Health Information."
Medical and Health Information	Any information concerning physical or mental health conditions or disabilities. Includes: - Medical record number - Health plan beneficiary number - Medical device identifiers and serial numbers - Prescription (Rx) number

	5. Health insurance identification or account number 6. Medical treatment – Information about the management and care of a patient or the combating of disease or disorder. 7. Medical diagnosis 8. Medical history 9. Medical payment information 10. Medical claims data 11. Medical images and metadata 12. Drugs, therapies, or medical products or equipment used 13. Family health or morbidity history - an account of all medical events and problems experienced by members of the individual's family 14. Other medical and health information
Genetic Information	Includes: Information about an individual's genetic tests. Excludes: Full DNA (see Biometric Data).

4.6 Customer Privacy

Data Element	Description
Customer Web Browsing and Search History	Includes: 1. Information about what searches DIRECTV customers perform 2. Web sites DIRECTV customers visit 3. Web pages DIRECTV customer's view 4. DIRECTV applications customers use on a DIRECTV Network (wireline and wireless including Wi-Fi) Excludes: 1. Searching, browsing, and activities associated with customers' use of official DIRECTV corporate web sites (e.g., any web sites that are resolved directly to, or redirect to, *att.com, *cricketwireless.com). <i>Note:</i> Exclusion from this row does not preclude potential pre-classification in another data element (e.g., customer viewing history). 2. History was captured at the network level prior to processing (e.g., raw data streams not associated with a customer).
Customer Viewing History	Information about programs watched or recorded, games and applications used, etc.
Customer Web Communications Payload - DIRECTV Use	When captured as part of service analysis, e.g., Deep Packet Inspection (DPI) data.

***Footnotes:**

Where a data element has the term "Subject to non-U.S. jurisdiction" associated with it, that data element is to be classified as DIRECTV Proprietary (SPI) when applied to data elements subject to the non-U.S. jurisdiction, irrespective of whether the data is created, handled, processed, destroyed, or sanitized inside or outside of the United States.

5.0 Table 2 - DIRECTV SCD Data Elements

Data elements in the following table must be treated as SCD when used in their entirety, unless explicitly stated otherwise. This applies to all data formats including scanned images, screen captures and recordings, PDFs, JPGs and any other unified communication, and collaboration tools/content.

5.1 SCD (Customer Privacy) – Involving Personally Identifiable Information

Data Element	Description
Customer data belonging to a customer of DIRECTV and requires a higher level of protection	All customer data that is identified as or should reasonably be known to be Sensitive Customer Data. Unauthorized disclosure would require notification of government agencies, individuals, or law enforcement; could expose individuals to a risk of physical harm, fraud, or identity theft; or could result in the loss of intellectual property.
Customer “messaging” content	Includes: Email, text messages, conference call recordings, and voice mail call recordings. Excludes: “Messaging” between customers and DIRECTV.
Customer Telemetry Data Customer Use	Automated communications for monitoring by the customer (rather than DIRECTV). Including all data that is generated by DIRECTV’s customers’ use of the Digital Life® service or any other Internet of Things (IOT) service that is used by the customer to monitor or control the service. For example, video files.