Identity, Access and Privileged Access Management (IAM) Services

1. General

1.1 IAM Services

The IAM Service provides a 24 x 7 real time identity and access management service using a combination of technology and skilled analyst to assist Customer with managing access to their systems. Level One, Level Two and Level Three support are in scope for this Schedule. This schedule ("Schedule") describes the IAM Services, the responsibilities of Customer and Accenture with respect to such services and terms and conditions applicable thereto. In the event of any conflict or inconsistency between this schedule and the Customer agreement with Verizon under which IAM Services are provided to Customer (the "**Customer Agreement**"), notwithstanding anything to the contrary in the Customer Agreement, the terms of this Schedule will control including with respect to descriptions, features and performance of the IAM Services set forth therein. For purposes of this Schedule, IAM Services means the Managed IAM with Accenture Services.

The IAM Services may include one or more of the following types of Services, each of which may be purchased by the Customer separately as specified in a Service Order:

(a) Identity Governance and Administration Services ("**IGA**")
(b) Privileged Access Management ("**PAM**")
(c) Access Management ("**AM**")

1.2 **Scope**. Accenture will provide the IAM Services for the Service Commitment using a global delivery model. Support is provided 24 x 7 from global delivery centers.

2. Identity Governance and Administration Services (IGA Services)

2.1 Solution Overview

IGA Service centralizes and automates the administration of User access to systems, Applications and resources, and allows Users to register their identities and manage their passwords and profiles across all integrated Applications. The centralized suite of IGA Services provides consolidated storage and management of User identities, policies and audit log information on who has access to which Applications and related data. Accenture will provide the IGA Services through a multi-tenant Okta IGA platform provided by Accenture (the "**IGA Platform**"). Each Customer is provisioned with a dedicated and isolated instance of the IGA Platform. All configurations, user data, and reporting are maintained within a separate portal and web link specific to the Customer. Customer will receives a unique, customized web link (e.g., <<customername>>.okta.com), configured exclusively for its organization. "**User**" means an employee, supplier, or contractor of Customer. "**Application**" means the applications supported as part of the Services listed in this Schedule.

IGA Services provide a set of basic capabilities (basic service elements) which are bundled into the Service. The basic Service elements are:

- Application and User onboarding into the IGA Platform and management
  - Onboarding includes the provisioning of Customer in the IGA platform and the granting of User access with the proper permissions and roles defined for each Application in scope, placing that Application under the control of the Customer identity governance process. Accenture will monitor the performance and troubleshoot issues, and confirm that Customer Applications are communicating with Accenture's IGA Platform.
- Identity Provisioning
  - Identity Provisioning provides for the creation and deletion of identities incorporating the Customer provided approval steps.

- The Service comprises the creation, changes or deletions of User identities to be routed through an approval process in accordance with the Customer's policies. Decisions with respect to these requests can be logged and stored.

- Workflow configuration & Management
  - The Service provides for workflows to be built within the IGA Platform in accordance with Customers provisioning process and associated approval requirements. These workflows can be created, updated, managed and retired to address changes to Customer policies and Applications.
- Identity and Role Mapping
  - The Service enables Customer to map the identities assigned to a common User across the set of Applications with the central and common identifier stored within the IGA Platform. This requires mapping to roles and tasks in the workflow. Recertification and segregation of duties specification and configuration is scope for in the IGA Services. The Service allows for a given User to be mapped across target Applications linked to the IGA Platform.
- Identity Logging
  - The Service enables identity provisioning and de-provisioning activities such as identity creation, changes, deletions, and approvals to be recorded within the IGA Platform. This provides the necessary accountability information for the type of activity that occurs for any given identity or Application.

2.2 **Service Descriptions**

Accenture will configure the IGA Platform environment and onboard Applications and configure workflows for the Customer.

2.3 **Applications**

Customers will be required to enable access to Customer environments to onboard and integrate with the IGA Platform in accordance with Accenture provided specifications. Only the following Customer Applications may integrate with the IGA Platform, unless otherwise agreed in the applicable Service Order:

- Active Directory synchronization
- LDAP synchronization
- Applications that can integrate using OOTB connectors, where "OOTB" means out-of-the-box; capabilities delivered by or within the standard software without configuration or change
- Log streaming
- ServiceNow ticketing
- SCIM compliant apps
- CSV connector
- HRMS

2.4 **Workflows**

Workflows will be created by Accenture for the following processes:

- Joiner/mover/leaver ("**JML**") process setup
- Recertification process per Application
- Birthright access provisioning
- Access approval workflow

2.5 **Reports**

Accenture will provide weekly OOTB reports on the number of identities and Applications managed, and Customer specific Service Level status across operations and configured workflows.

2.6 **IGA Service Operations**

Accenture will provide operational support for the IGA Services including the IGA Platform.

3. **Privileged Access Management ("PAM")**

3.1 **Solution Overview**

Accenture PAM Services assist Customers in managing access for privileged identities for privileged accounts. PAM capabilities enable consistent, policy-based security controls for privileged User behavior and the monitoring, detection, and prevention of unauthorized privileged access to critical Customer resources. PAM follows the principle of least privilege, providing Users with the minimum necessary access required to perform their role tasks. Accenture will provide the PAM Services for the Customer in a client dedicated environment (i.e., a single tenant environment) on the Okta Privileged Access platform ("**PAM Platform**"). Licensing of the PAM Platform will be managed and maintained by Accenture. Each Customer is provisioned with a dedicated and isolated instance of the PAM Platform. All configurations, user data, and reporting are maintained within a separate portal and web link specific to the Customer. Customer will receives a unique, customized web link (e.g., <<customername>>.okta.com), configured exclusively for its organization.

- Accenture PAM services comprise:
  - Onboarding which includes the provisioning of privileged accounts to grant access with the Customer permissions and roles defined for each Application in scope.
  - Ongoing Support. Confirming that the underlying technology is functioning appropriately, maintaining and monitoring the performance of the Application and troubleshooting issues, and confirming that the Customer Applications are integrated with the PAM Platform.
- Identity Logging
  - Privilege account creation, changes, deletions, and approvals are appropriately captured and stored within the PAM Platform. This provides the necessary accountability information for the type of activity that occurs for any given identity or Application.

3.2 **Service Descriptions**

The PAM Service comprises the following:

3.2.1 Onboarding of the following types of privileged accounts: local administrative accounts, Domain administrative accounts, PAM Service account, Active Directory or domain service accounts, and Application accounts.

3.2.2 Integration with the following Customer system types:

- Databases
- Domain Controller
- Servers
- Network Device
- Cloud
- workstations
- Active Directory ("**AD"**)

3.2.3 Provisioning accounts which will have access, as applicable for the Customer, to the Security Incident and Event Management ("**SIEM**"), the instance of the Google Chronicle or other supported platform, provided as a hosted service.

3.2.4 Just-in-time access management

3.2.5 PAM application management

3.2.6 Prebuilt integrations for specific set of reports (Service Level / MTTR)

3.3 **Activities**

The PAM Services comprise performing the following activities in accordance with the applicable Customer Service Order:

3.3.1 Manage enforcement of access policies for privileged administrators

3.3.2 Manage password rotations and unlock / unsuspend of privileged Users

3.3.3 Support password change activity service

3.3.4 Resolve account on-boarding, account off-boarding, tickets related to User issues and problems

3.3.5 Perform Start/Stop/Restart of the in-scope PAM Application components as required.

3.3.6 Update User, operations documentation, and knowledge management database including lessons learned for continuous service improvement.

3.3.7 Resolve incidents related to Customer integrations with problem management and root cause analysis

3.4 **Reports**

Accenture will provide OOTB weekly reports on the number of user accounts with elevated access to sensitive data and critical systems within an organization ("**Privilege Accounts**") and Applications managed, and Customer Specific Service Level status across operations and configured workflows.

4. Access Management ("AM")

4.1 Solution Overview

Accenture Access Management Services include enabling:

- Access to identified Applications for single sign on ("**SSO**") integration: Support integrations with all key applications identified by the Customer, including SaaS, and web Applications.
- SSO customization: providing the User visibility of only the Applications they have permission to access.
- Multifactor Authentication (MFA) integration: MFA, enabled for those Users using Phone or email channels to access Applications.
- Monitoring and troubleshooting.

Accenture will provide AM Services, provided on the Okta platform, using the multi-tenant AM platform ("**AM Platform").** Licensing of the AM Platform will be managed and maintained by Accenture. Each Customer is provisioned with a dedicated and isolated instance of the AM Platform. All configurations, user data, and reporting are maintained within a separate portal and web link specific to the Customer. Customer will receives a unique, customized web link (e.g., <<customername>>.okta.com), configured exclusively for its organization.

4.2 Service Descriptions

The AM Platform is configured to provide the following capabilities in accordance with the Customer's internal security and system access policy and process:

- Foundation setup for access management
- Access policy configuration
- Configure risk-based authentication policies
- Enable custom domain for tenant
- Active Directory authentication integration
- Active Directory agent integration
- External Identity Provider (IdP) integration
- Multi-factor authentication
- Application onboarding with SAML (Security Access Markup Language) /OIDC (OpenID Connect) and HTTP Header injection
- Application assignment to Users
- User onboarding from Active Directory or import
- User interface branding to update the login pages
- Enable self-service password reset and registration
- Log streaming to SIEM

4.3 **Activities**

In order to integrate the AM Services, the following activities shall be performed in accordance with the applicable Customer Order:

- Create Policy Framework by configuring SignOn Policy, MFA Enrollment Policy, Password policy for Applications
- Onboarding of Customer Users for the AM Services will comprise enabling the following Platform capabilities in accordance with the applicable Customer Service Order:
  - Manage enforcement of authentication and authorization policies
  - Resolve Account On-Boarding
  - Account Off-Boarding and tickets related to User Issues
  - Perform Start/Stop/Restart of the in-scope AM services as required.
- Resolve incidents related to Customer integrations performing problem management and root cause analysis.

4.4 **Reports**

Accenture will provide OOTB weekly reports on the number of Users and Applications managed, and Customer specific Service Level status across operations and configured workflows.

5. **Ongoing Activity Responsibility Matrix (IGA, PAM and AM Services)**

IDENTITY MANAGEMENT		
Responsibility	**Accenture**	**Customer**
SET UP AND ONBOARDING ACTIVITIES		
Provide a Single Point of Contact (SPOC) to provide all information required for provisioning the platform, connectivity, and integrations. In addition, the SPOC will facilitate the testing and sign off for the commencement of the applicable Services. The SPOC will be responsible for internal communication to Customer's users.		X
Provide access and Ids to Accenture personnel for Customer Applications identified for onboarding (Test, QA and Prod) environments		X
Provide list of identity management rules specifically for Identity Governance Segregation of Duties ("SOD"), Roles and accesses, and relevant Policies for IGA and PAM		X
Define communication protocol to Customer's users and provide to Accenture		X
Approve set up and service commencement timeline and ensure timely availability and completion of any changes required in the Customer's Applications		X
Identify customization needs and change processes or workarounds	X	
Agree/Approve on change processes or workarounds		X
Create cut over plans for Service commencement	X	
Provide approval for service commencement		X
Execute Application side changes for onboarding into AM/IGA/PAM Platform		X
Develop system testing plans	X	
Execute end to end system testing and inform Customer on the tasks assigned to them for system testing	X	
Participate in the system testing on the tasks assigned to Customer in accordance with the system test plans		X
Execute changes to Applications as needed, basis system testing observations		X
Resolve issues related to the AM /IGA/PAM Platform to mitigate issues discovered during system testing	X	
LEVEL ONE SUPPORT SERVICES		
Level One support provided via a 1-800 number	X	
Assist Users in recovering or resetting their passwords	X	

Help Users regain access to locked accounts	X	
Guide Users through the process of enrolling in MFA	X	
Assist Users in re-enrolling in MFA when required	X	
Troubleshoot and resolve synchronization problems with MFA	X	
Help Users generate or use backup codes for MFA	X	
Assist Users in transitioning to alternative MFA authentication methods	X	
Resolve compatibility problems between browsers or devices and IAM systems, which include the IGA Platform, AM Platform, and PAM Platform	X	
Help Users access Applications when login problems occur	X	
Assist Users with resolving issues where Users are denied access to Applications	X	
Provide updates on the status of access requests	X	
Assist Users in updating incorrect language preferences	X	
Assist Users with modifying inaccurate personal details in IAM systems, which include the IGA Platform, AM Platform, and PAM Platform	X	
Identify and resolve issues or problems causing slow system performance	X	
Troubleshoot and escalate issues to Level Two support	X	
LEVEL TWO SUPPORT SERVICES		
Provide Application specific data and personnel to execute recertification process		X
Monitor execution of daily, weekly and monthly actions generated by Customer's authoritative feeds	X	
Ensure that the Customer authoritative feed is always up to date and that the data is appropriate. Remedy any issues with the authoritative feed and/or the data		X
Troubleshoot and Resolve issues with metadata associated with a specific User ID (e.g., Name, Email ID, Enterprise employee ID) ("User Data") if errors occur during feed processing and automated provisioning/de-provisioning	X	
Troubleshoot and escalate issues to Level Three support if errors occur during feed processing and automated provisioning/de-provisioning due to Application integration issues	X	
Troubleshoot and escalate issues to Level Three support if errors occur due to workflows for approvals, SoD rules and roles configured within the Identity Management system	X	
Perform remediation activities for provisioning/User terminations if errors occur during feed processing	X	
Trigger and track certification campaigns	X	
Track remediation of outcomes from the access certification activity	X	
Supporting and administration of all reporting and recertification campaigns	X	
Resolve User related issues as per agreed upon Service Levels	X	
Monitor and collect technical capacity statistics on a monthly basis related to Users provisioned, Users de-provisioned, self-service requests, and incidents resolved	X	

Analyze Identity Management Solution capacity statistics	X	
LEVEL THREE SUPPORT SERVICES		
Provide list of identity management rules		X
Approve technical changes assigned to Level Three		X
Resolve issues with respect to policy violations for Access policies, provisioning policies and reconciliation policies	X	
Execute changes required to Customer applications to resolve issues		X
Identify opportunities for improvement of workflows	X	X
Provide resolution of issues with respect to the configuration of recertification campaigns	X	
Work with Customer stakeholders to identify and configure the right SoD rules	X	
Execute approved technical changes assigned to Level Three	X	
Qualify technical tickets directly routed to Level Three	X	
Problem Investigation & Diagnosis-Severity 1 / Critical Tickets	X	
Problem Resolution & Recovery-Severity 1 / Critical Tickets	X	
Participate in Root Cause Analysis of Severity 1 / Critical Tickets	X	
Incident Investigation & Diagnosis-Severity 1 / Critical Tickets	X	
Incident Resolution & Recovery-Severity 1 / Critical Tickets	X	
Plan technical approach for applying required Application fixes	X	
Schedule technical corrections (i.e., bug fixes) provided by the technology vendor into the monthly release schedule	X	
Coordinate the remediation of technical incident tickets with technology vendors	X	
Deploy fixes/changes as part of monthly release schedule	X	
Maintain Customer vendor support access information (e.g., password to vendor website, contracts, etc.)		X
Coordinate with Level Two and change management team for monthly release deployments to the Applications that have been approved by the Customer	X	
Integrations		
Support the Customer's integration of new Applications into the applicable IAM Platform – as defined in the service description following the fixed integration pattern approach (SAML / OIDC/AD Entitlement)	X	
Advise Accenture if Customer wishes to integrate new Applications into the Identity Management System (unless otherwise agreed in a change order)		X
Implement new Applications into the Identity Management System were agreed with Customer	X	
Enhancements and other changes		
Estimate the scope and effort required for changes to Services requested by Customer	X	
Approve the effort & scope required for changes		X
Analyze and review the change order	X	
Propose time and cost estimate for the change	X	
Accept proposed time and cost estimate for the change		X
Build implementation, testing and roll out schedule basis mutually agreed timeline, cost and process	X	
PLATFORM SUPPORT		
System Performance Monitoring		
Monitor availability and performance of the IAM platforms (IGA, AM or PAM) using health checks, and follow-up with corrective actions or escalations in case of unavailability or low performance	X	
Patch Management for the Identity Management Solution		
Identify, analyze and prioritize patches	X	

Conduct testing for each patch	X	
Follow Change/Release management process	X	X
Inform Customer of possible downtime	X	
Disaster Recovery		
Develop and maintain disaster recovery plan in partnership with Platform provider	X	
LICENSE		
Obtain and Maintain Licenses related to the Identity Management Solution, Access Management Solution and PAM Solution.	X	

5.1 **Out of Scope**

The following activities are not in-scope of the IAM Services:

- Vulnerability Management scanning of Customer applications
- Remediation of operating system related vulnerabilities and patching
- Desktop Applications are considered out of scope for "SSO" configuration Database installation and upgrades, data conversion and migration
- Training for end Users and provision of web-based training material
- Resolution of data issues within the source or target systems
- Any code/configuration changes in any Customer systems/Applications
- Assessment or review of Customer's existing IT policies, standards or guidelines or making updates or providing
- Recommendations for change in respect of the same
- Multi-lingual support
- Role mining or Role management
- Development of custom components and/or custom integrations unless otherwise agreed in the applicable Customer Order
- Reporting outside of those defined in this Schedule
- Audit support
- Custom workflows Deployment of infrastructure in Customer environments

6. **Service Levels**

PRIORITY LEVEL	DEFINITION	INDICATIVE RESPONSE TIME	MAXIMUM RESOLUTION TIME	COVERAGE WINDOW	TARGET RESOLUTION	MINIMUM RESOLUTION
1	Business process and system functionality have been severely impacted or halted. A successful attack has rendered the system(s) or system data unsafe, inoperable, or compromised.	30 Minutes	4 Hours	24x7	95%	90%
2	Business process and system functionality have been seriously affected. Systems and/ or system data are exposed to interruption, compromise, or loss.	60 Minutes	8 Hours (within service hours)	24x7	95%	90%
3	Business process and system functionality may be moderately affected. A threat may exist against systems or system data.	4 Hours	3 Business Days	varies	95%	90%
4	Systems and/ or system data are not at risk. These events are required for purposes of auditing, forensics, and legal or regulatory compliance, and may also be useful for trend analysis or correlation. The Informational	24 Hours	8 Business Days	varies	95%	90%

	severity level serves as the default for unclassified events.					

Automated responses from the service desk/ticketing tool are permitted for calculating the response time Service Level.

Under the following circumstances the Service Levels shall not be applicable.

- a force majeure event
- No Customer response for further information or acceptance testing after three (3) attempts
- Required fix not available until future upgrade or major patching Release (e.g., Hotfix, Service Pack) from third party vendor
- Any failure to meet a designated service level because an unsupported product failed after Accenture notified the Customer of the product's impending status and the Customer elected not to upgrade the product to a supported version
- Any action or inaction by the Customer or their nominated third party that is the substantive cause of a failure to meet a designated Service Level

7. Collection and Processing of Customer Personal Data

7.1 Acknowledgement

Customer acknowledges that in providing the IAM Services, Accenture may, on behalf of Customer, collect, process and store certain information relating to an identified or identifiable natural person, as provided by the applicable Data Protection Laws ("**IAM Personal Data**"). The: (i) subject matter and duration of the processing; (ii) nature and purpose of the processing; and (iii) type of IAM Personal Data and categories of data subjects shall be as specified in Attachment 1 to this Schedule ("**Transparency Notice")**.

7.2 Sub-Processors

Customer authorizes Accenture to engage the Accenture Affiliates, and the third-party Sub-processors detailed in the applicable subprocessor list set forth in the Transparency Notice.

7.3 Data Controller

Customer acknowledges and agrees that it acts as a data controller for the processing of such IAM Personal Data and Accenture acts as a data processor under applicable Data Protection Laws. In certain cases, as further specified in the Transparency Notice, Accenture may also collect and process certain IAM Personal Data as a "**Controller**". Each party will comply with the requirements of the Data Protection Laws as applicable to such party with respect to the processing of IAM Personal Data.

7.4 Consents

Customer will ensure that it has and will maintain during the provision of the IAM Services, all necessary rights (including lawful legal basis (as applicable)) and permissions to provide the IAM Personal Data to Accenture for the processing to be performed in relation to the Service, and that Customer has provided all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the IAM Personal Data.

7.5 Data Safeguards

Accenture agrees that it will: (i) only use the IAM Personal Data to the extent that is necessary and proportionate to perform the IAM Services, and in accordance with Customer's instructions, and only for duration of the IAM Services; (ii) implement appropriate technical and organizational security measures to safeguard IAM Personal Data, as specified in Accenture's Data Safeguards ("**Data Safeguards**") published by Accenture at www.accenture.com/client-data-safeguards (or successor URL), with respect to which, Customer has satisfied itself that the Data Safeguards provide a level of security appropriate to the risk in respect of any processing of IAM Personal Data; (iii) provide assistance as reasonably requested by Customer with respect to Customer's obligations under applicable Data Protection Laws (e.g. responding to requests by individuals, providing notice of breaches, consulting with regulators); (iv) make available

information as reasonably requested by Customer to demonstrate Accenture's compliance with its obligations under this clause; and (v) return or destroy (at Customer's direction) such IAM Personal Data upon request of Customer or termination of the IAM Services, to the extent that any IAM Personal Data is retained by Accenture in performing the IAM Services, as specified in the Transparency Notice.

7.6 **Transfer**

For the purposes of delivering the IAM Services, IAM Personal Data may be transferred outside the country where IAM Personal Data originates from. Destination countries might not be recognized by an adequacy decision under the applicable Data Protection Laws. Accordingly, in order to protect IAM Personal Data being transferred to such countries in connection with the delivery of the IAM Services, Accenture adopts the transfer mechanism(s) as specified in the Transparency Notice.

7.7 **CCPA**

The following shall apply to the extent that the California Consumer Privacy Act ("**CCPA**") and/or the California Privacy Rights Act ("**CPRA**") applies. Accenture shall: (i) not sell or share any IAM Personal Data (as defined by CCPA and CPRA); (ii) not retain, use or disclose any such IAM Personal Data for any purpose other than business purposes specified in accordance with this Schedule; or (iii) not retain, use or disclose such IAM Personal Data outside the direct business relationship between Accenture and Customer, as set forth in this SOW, unless otherwise required by law; (iv) not process outside the specified business purpose; (v) provide the same level of privacy protection required by the applicable obligations under CPRA for IAM Personal Data received by Accenture; (v) not combine personal information of opted out individuals from the Customer with different sources or with data collected from its own interaction with consumer; (vii) notify the business if it can no longer meet its obligations under CPRA and will work with the business to take appropriate steps with regard to the IAM Personal Data. Customer agrees that execution of the applicable Service Order shall be deemed to constitute any certification that is required under applicable Data Protection Laws to the restrictions on sale, retention, use, or disclosure of IAM Personal Data.

8. **Terms Applicable to the IAM Services**

8.1 **Customer Assurances**

Customer: (i) explicitly confirms to Accenture that it has obtained all applicable consents and authority for Accenture to deliver the IAM Service; (ii) gives Accenture explicit permission to perform the IAM Services and to access and process any and all Customer data related to the Service; (iii) represents that such access and processing does not violate any applicable law, or any obligation Customer owes to a third-party. Customer shall fully indemnify and hold harmless Verizon and its providers from and against any claims by any third parties related to the Services.

8.2 **Compelled Disclosures**

Customer acknowledges and agrees that in the course of using the IAM Services, Accenture may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which Customer is subject to in one of more jurisdictions. Customer shall remain solely responsible for all such reporting requirements and Accenture shall have no liability in this regard, unless it is under an independent legal obligation to report, in which case Accenture will use reasonable endeavours to notify Customer in advance of responding to any such requirements and, if possible, will allow Customer the opportunity to raise an objection with such authorities.

8.3 **Performance Standard**

The IAM Services are provided as one element of the Customer's overall security control framework. Accenture will provide the IAM Services with due care and skill, but notwithstanding anything to the contrary in this Schedule, Customer acknowledges that the IAM Services are not guaranteed to: (i) detect or identify all security or network threats to, or vulnerabilities of Customer's networks or other facilities, assets, or operations; (ii) prevent all intrusions into or any damage to Customer's networks or other facilities, assets, or operations; or (iii) return control of Customer or third-party systems where unauthorized access or control has occurred.

8.4 **Remediation Recommendations**

Customer is solely responsible for assessing (and as applicable, implementing) any recommendations, advice and/or instructions provided by Accenture in the course of providing the IAM Services.

8.5 **Usage Information**

Customer acknowledges and agrees that Accenture and its licensors owns the statistical usage data derived from the operation of the IAM Services, including data regarding web Applications utilized in connection with the Services, configurations, log data, and the performance results for the Service ("**Usage Data**"). Nothing herein shall be construed as prohibiting Accenture and its licensors from utilizing the Usage Data to optimize and improve the IAM Services provided that if Accenture provides Usage Data to third parties, such Usage Data shall be de-identified and presented in the aggregate so that it will not disclose the identity of Customer to any third party.

8.6 **Updates to the Services**

Accenture may update any of the Services from time to time, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of such Services. Additionally, Accenture may make changes to the Service as required to comply with applicable law or to address a material security risk as advised by the underlying platform provider.

8.7 **Restrictions**

Customer will not send or store in the IAM Services (i) any personal health data, credit card data, personal financial data or other such sensitive data which may be, without limitation, subject to the Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, or the Payment Card Industry Data Security Standards; (ii) send or store infringing or unlawful material in connection with the Service; (iii) send or store viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs to the Service; (iv) attempt to gain unauthorized access to, or disrupt the integrity or performance of, the Service or the data contained therein; (vi) modify, copy or create derivative works based on the Service, or any portion thereof.

8.8 **License**

Customer grants to Accenture, its Affiliates and applicable licensors and contractors a worldwide, limited-term license to host, copy, transmit and display Customer data, as reasonably necessary for Accenture to provide the Service in accordance with this Schedule.

ATTACHMENT 1 -TRANSPARENCY NOTICE –

Revision Date: December 1, 2024

This Transparency Notice describes how Accenture's IAM Service collects and processes personal data. For the purposes of this Transparency Notice, "**Accenture**" shall mean the Accenture entity that has entered into an agreement with Verizon.

IAM SERVICE – OVERVIEW
The IAM Services are a managed security service comprising: a multi-tenant instance of Okta's hosted IAM software for IGA and AM Services, and a dedicated instance of Okta for PAM.

PERSONAL DATA, COLLECTION & PROCESSING
DATA PRIVACY – ROLES OF ACCENTURE AND CUSTOMER. With respect to personal data that Accenture is required to process to deliver the IAM Services, the Customer acts as the 'Controller', and Accenture acts as a 'Processor', as further detailed in the section 'Collection & Processing – Customer-Controlled Personal Data' below.

COLLECTION & PROCESSING – CUSTOMER-CONTROLLED PERSONAL DATA. The rights and obligations of Accenture and the Customer with respect to the processing of Customer-controlled personal data are specified in the Schedule. The following table details the personal data that Accenture collects, processes and stores on behalf of a Customer, the applicable data subjects and the nature and purpose of processing.

NOTE: Accenture has no control over the content of the personal data processed by Accenture in delivering the IAM Service on behalf of a Customer:

CATEGORY	PERSONAL DATA	DATA SUBJECTS	NATURE AND PURPOSE
Customer Care Data*	● Personal data contained in a Customers request for support through chat, email, voicemail, SMS/MMS (NOTE: Personal data may include Security Data (see below) processed by Accenture in connection with the provision of the IAM Service, as may be required for Customer to detail its request and for Accenture to action such request for support e.g., location data, network activity data, authentication data).	Customers personnel, customers, suppliers, and any persons interacting electronically in or with Customer's networks.	Personal data stored and processed by Accenture, in order to provide technical support to Customers during their use of IAM Service.
	● Personal Data contained in security events and activity logs e.g., IP Address, Email Address, MAC Address, Host, Usernames, Device IDs and similar Unique Identifiers, Event ID, Process ID, Machine ID, WAP and/or Web Logs Files, Browsing Logs, Session Logs, Location Data (device and network locale).	Customer's personnel, customers, suppliers, and any persons interacting electronically in or with Customer's networks.	

*NOTE: The personal data indicated above is NOT expected to include Special Categories of personal data.

DURATION OF PROCESSING OF CUSTOMER-CONTROLLED PERSONAL DATA. Customer-controlled personal data will be retained by Accenture for the duration of a Customer's Service Commitment to the applicable IAM Service. Following the expiration or earlier termination of a Customer's Service Commitment, or at a Customer's request, Accenture will (and will require that its Sub-processors) promptly and securely delete (or return to the Customer) all personal data (including existing copies), unless otherwise required or permitted by applicable laws. Unless otherwise agreed, Accenture will comply with a Customer's deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.

SUBPROCESSSOR LIST –

IAM Services

Revision Date: December 2024

IDENTITY AND ACCESS MANAGEMENT SERVICES. Accenture engages data processor(s) ("**Subprocessor(s)**") to support the delivery of Accenture's Identity and Access Management Services ("**IAM Service**").

ACCENTURE AFFILIATE SUBPROCESSOR(S). Accenture engages one or more of the affiliates listed below as a Subprocessor(s) with respect to the IAM Service:

Delivery – Staffing Locations

The IAM Services for Customers headquartered in the United States will be provided by one or more of the following Accenture affiliates in the following jurisdictions.

ACCENTURE AFFILIATE	COUNTRY	IAM SERVICES
Accenture Solutions Pvt. Ltd	India	Global SOC 24x7x365
Accenture LLP	USA	Service Delivery Lead (8 X 5 business hours)

THIRD PARTY SUBPROCESSOR(S). Accenture currently uses the following third-party Subprocessor(s) to provide certain services, as detailed in the table below, necessary to deliver IAM Service to Customers headquartered in the United States. Prior to engaging any third-party Subprocessor(s), Accenture performs due diligence to evaluate a Subprocessor(s)' privacy, security and confidentiality practices, and executes an agreement implementing its applicable obligations with each Subprocessor(s), including Standard Contractual Clauses to cover any international data transfer as required under applicable data protection laws.

THIRD PARTY SUBPROCESSOR(S)	SERVICES PROVIDED AND RELATED PURPOSE	COUNTRY / REGION WHERE DATA IS PROCESSED
Okta, Inc. and the following subprocessors as may be updated by Okta at: www.okta.com/trustandcompliance/#subprocessorinformation	IAM Platform and software capability to perform the IAM Services.	USA

Delivery – Staffing Locations

The IAM Services for Customers headquartered in Australia, United Kingdom, Germany, Japan, France, Netherlands, Switzerland, Finland, Norway, Italy, Belgium, Ireland, Sweden, Spain, Luxemburg, Austria, Denmark and other agreed-upon countries will be provided by one or more of the following Accenture affiliates in the following jurisdictions.

ACCENTURE AFFILIATE	COUNTRY	IAM SERVICES
Accenture Solutions Pvt. Ltd	India	IAM Support 24x7x365 Service Delivery Lead

Accenture LLP	USA	Service Delivery Lead (8 X 5 U.S. business hours)

THIRD PARTY SUBPROCESSOR(S). Accenture currently uses the following third-party Subprocessor(s) to provide certain services, as detailed in the table below, necessary to deliver IAM Service to Customers headquartered in Australia, United Kingdom, Germany, Japan, France, Netherlands, Switzerland, Finland, Norway, Italy, Belgium, Ireland, Sweden, Spain, Luxemburg, Austria, Denmark and other agreed-upon countries. Prior to engaging any third-party Subprocessor(s), Accenture performs due diligence to evaluate a Subprocessor(s)' privacy, security and confidentiality practices, and executes an agreement implementing its applicable obligations with each Subprocessor(s), including Standard Contractual Clauses to cover any international data transfer as required under applicable data protection laws.

THIRD PARTY SUBPROCESSOR(S)	SERVICES PROVIDED AND RELATED PURPOSE	COUNTRY / REGION WHERE DATA IS PROCESSED
Okta, Inc. and the following subprocessors as may be updated by Okta at: www.okta.com/trustandcompliance/#subprocessorinformation	IAM Platform and software capability to perform the IAM Services.	USA/European Union