PowerPlan Security Policy

Version 2.1

Last Revised April 2021

Table of Contents

Introduction to the PowerPlan Security Policy

The purpose of PowerPlan's Security Policy (the "Policy") is to reflect PowerPlan's commitment to protecting your Hosted Data and the processes, procedures, and protections it has designed and implemented with respect to its SaaS, Cloud Services, and Subscription Services in support of that commitment.

All references to "you" or "your" refer to the Client pursuant to an executed and currently active Order Form for SaaS, Cloud Services, or Subscription Services.

To align with then current industry standards and to align known and emerging risks, PowerPlan may update this Policy from time to time. The version available at https://info.powerplan.com/SecurityPolicy will apply to your SaaS, Cloud Services, or Subscription Services, as applicable. You should check regularly for updates.

Definitions:

1. Cloud Services means the services provided by PowerPlan to make the Hosted Software available through use of the Platform.
2. Hosted Data means the data that an Authorized User loads into, processes, or stores using the SaaS, Cloud Services, or Subscription Services.
3. Hosted Software means the user interface, the underlying database, data architecture, data model, data schema, and data structure, and the object code version of the software identified on the Order Form, including all Modifications provided by, or granted access to, by PowerPlan to Client from time to time, which is made available remotely over the Internet via Subscription Services or as part of the SaaS, or is otherwise licensed from PowerPlan and made available through Cloud Services.
4. Maintenance Policy refers to the maintenance policy that is applicable based on the PowerPlan offering procured by Client. For SaaS, this means the PowerPlan Standard Maintenance Policy for SaaS available at https://info.powerplan.com/SaaSMaintenancePolicy. For Cloud Services, this means the PowerPlan Standard Maintenance Policy for Perpetual Licenses available at https://info.powerplan.com/PerpetualLicenseMaintenancePolicy. For Subscription Services, this means the PowerPlan Standard Maintenance Policy for Subscription Services available at https://info.powerplan.com/SubscriptionMaintenancePolicy.
5. Maintenance Services means the support and maintenance services provided by PowerPlan per the applicable agreement between you and PowerPlan, including PowerPlan's then-current Maintenance Policy.
6. Multi-Instance refers to the Solution Platform which provides a unique database per client with a shared application instance.
7. Multi-Tenant refers to the Solution Platform which provides a shared database and application instance.
8. Platform means the information technology infrastructure, including computers, servers, hardware, databases, database management systems, networks, communications infrastructure, devices, websites, and third-party software used by PowerPlan to provide access to the Hosted Software as part of the SaaS or through the Cloud Services or Subscription Services.
9. Professional Services means the installation, implementation, training, consulting, and other services provided by PowerPlan in accordance with a statement of work or otherwise billed on a time and materials basis.
10. SaaS means Software as a Service and includes the Hosted Software, Platform, applicable documentation, and associated Maintenance Services, as indicated in the applicable agreement between you and PowerPlan. For the avoidance of doubt, Professional Services are not a component of SaaS.
11. Single-Tenant refers to the Solution Platform which provides a unique database and unique application instance per client.
12. Solution Platform refers to the method in which a Hosted Software module is structured and operationally controlled within the hosted environment.
13. Subscription Services means (i) the services that allow Client to utilize the Platform operated and maintained by PowerPlan to access and use the Subscribed Products during the Subscription Term, and (ii) the Maintenance Services. For the avoidance of doubt, Professional Services are not a component of Subscription Services.

Personnel:

1. All personnel will undergo criminal background checks at the time of hire. PowerPlan may conduct additional background checks in its discretion based on the individual's specific role within PowerPlan.
2. PowerPlan will contractually obligate all personnel to avoid inappropriate use or disclosure of the confidential information of PowerPlan and its clients as a condition of employment.

3. Personnel must follow with PowerPlan's policies which have been designed in accordance with ISO27001 standards and cover:
    a. Categorization of all data based on the sensitivity levels of information and form or media through which it is accessed;
    b. Appropriate access, use, and retention controls and processes according to the categorization of data as noted above;
    c. Acceptable use of the IT assets and network used by PowerPlan; and
    d. Account and password management;

   PowerPlan's security team will review such policies no less often than annually.
4. PowerPlan will train all personnel on above referenced security policies and procedures, no less often than annually.

Data Center:

1. PowerPlan will utilize a SOC 1 and SOC 2 certified data center to store your Hosted Data.
    a. To be compliant with SOC 1 and SOC 2 requirements, the Data Center will maintain controls related to:
        i. Physical Protections of the Data Center (including security, cameras, backup power sources, etc.);
        ii. Technical Infrastructure Security (including firewalls and encryption at rest and in transit); and
        iii. Authorized User Identification and Access Management (including authentication requirements)
2. Monitoring: The data center service provider will monitor its data centers for availability 7 days a week, 24 hours a day.
3. Redundancy and Backups (Production Instance Only):
    a. Production environments will be configured in redundant environments in geographically distant zones to support the service level targets as well as the backup and recovery obligations noticed in this document.
    b. Backup and recovery model which permits point in time recovery up to thirty-five (35) days
    c. In addition, PowerPlan conducts the following backups:
        i. Daily backups (kept for seven (7) days),
        ii. Weekly backups (kept for five (5) weeks),
        iii. Monthly backups (kept for thirteen (13) months
        iv. Annual backups (kept for three (3) years)
4. For Single-Tenant Solution Platforms, Client may select one the following regions to store the Hosted Data:
    a. United States
    b. Canada
    c. Australia
    d. European Union

   For Multi-Instance and Multi-Tenant Solution Platforms, the United States data center region will be used to store the Hosted Data.
   PowerPlan will not transfer your Hosted Data out of such region without written consent from your System Administrator, provided that:

    a. You notify PowerPlan of your selection no less than thirty (30) days before the start of the applicable SaaS, Cloud Services, or Subscription Services understanding that subsequent requests to move geographic locations may incur additional fees;
    b. You are solely responsible for ensuring that PowerPlan has all appropriate rights and consents to store the Hosted Data in the selected region; and

c. PowerPlan may access, although not store, Hosted Data from outside of the selected jurisdictions, subject to the limitations contained in the Use of Hosted Data section below.

Use of Hosted Data:

PowerPlan may only store, modify, use, or process Hosted Data to:

1. Fulfill PowerPlan's obligations (including taking actions reasonably related to such obligations, such as receiving, storing, archiving, copying, retrieving, processing, using and transmitting Hosted Data, as applicable) under an active agreement between you and PowerPlan, which without limitation includes:
    a. Delivery of or access to SaaS, Cloud Services, or Subscription Services in accordance with an active Order Form executed by You and PowerPlan
    b. Maintenance Services provided as part of the SaaS, Cloud Services, or Subscription Services in accordance with the Maintenance Policy, if applicable
    c. Security obligations under this Policy or the Acceptable Use Policy
    d. Uptime obligations under the Service Level Policy
    e. Delivery of Professional Services in accordance with a statement of work or other agreement for services executed by you and PowerPlan

    PowerPlan may also provide access to the Hosted Data to a data center provider, cloud computing platform provider, or other permitted third-party, subcontractor, or subprocessor, but solely to the extent necessary for reasonable support of the permitted uses under this Data Use Section and subject to confidentiality obligations.
2. Follow (including taking reasonable steps in furtherance of the parties' compliance with) any applicable law, statute, regulation, ordinance, or contract.
3. Modify, improve, or further develop PowerPlan's SaaS, Cloud Services, or Subscription Services offerings (including any components of such services such as the Hosted Software, the Platform, and Maintenance Services, collectively or individually) and Professional Services.
4. Aggregate Hosted Data and data with content and data from other clients ("Data Aggregations") for purposes including, without limitation, product and service development and commercialization and quality improvement initiatives. PowerPlan will redact Hosted Data in such a way as to not divulge Client's Confidential Information. All Data Aggregations will be the sole and exclusive property of PowerPlan, provided that nothing in the foregoing is intended to reduce or diminish Client's rights to its Confidential Information and Hosted Data, which right remain exclusively with Client.

Except as permitted in accordance with this Section or as otherwise agreed upon in writing by you and PowerPlan, PowerPlan will not sell or lease your Hosted Data, nor otherwise enter into any commercial transaction for access to your Hosted Data with any third-party.

Security Scans and Tests:

PowerPlan will conduct the following tests and scans on the SaaS (and Cloud Services and Subscription Services, as applicable), no less frequently than the frequency noted below:

1. OWASP Top 10 Scans on the Hosted Software - Annually
2. Penetration Testing on Platform - Annually
3. Vulnerability Scans on Platform – Quarterly
4. Virus/Malware Scans on Platform and Hosted Software – In Real-Time

In the event any vulnerabilities are discovered through such testing, PowerPlan will use commercially reasonable efforts to resolve such vulnerabilities in a timely manner, using the processes and procedures supported by industry standards such as SOC 1, SOC 2, or ISO 27001 as applicable.

Change Management:

For Single-Tenant Solution Platforms, PowerPlan will not perform any of the following functions on the production instance of the Hosted Software without your written consent:

- Apply a PowerPlan Hosted Software Release
- Modify Hosted Data within the Platform with a script, or
- Implement any custom code or configuration to remediate an issue preventing you from meeting your internal accounting or reporting requirements or deadlines

Such changes may also be generally referred to as Customer Initiated Changes (CIC).

For Multi-Instance and Multi-Tenant Solution Platforms, PowerPlan will not perform any of the following functions on the production instance of the Hosted Software without your written consent:

- Modify Hosted Data within the Platform with a script

Such changes may also be generally referred to as Customer Initiated Changes (CIC). For non-emergency changes, PowerPlan will deploy the changes to production Monday-Wednesday, 8:00 am-5:00 pm EST after receiving Client approval for deployment. PowerPlan will deploy emergency changes to production as needed after receiving Client approval for deployment.

PowerPlan may implement the following changes to the Hosted Software and Platform (including any related systems, networks, and environments) without your written consent:

- Emergency (Break/Fix Change) (EC): A change that must be implemented as soon as possible to restore service, avoid a service disruption, or avoid a critical security risk, provided that PowerPlan will provide notice once reasonably practicable in the event this type of change is necessary.
- Standard Change (SC): A pre-authorized change that is low risk, relatively common and follows a procedure or work instruction (e.g. – operating system patches) or changes which are not likely or intended to modify the calculations performed on your Hosted Data by the Software.
- Multi-Instance/Multi-Tenant Solution Platform Change (MPC): For Multi-Instance and Multi-Tenant Solution Platforms only, apply a PowerPlan Hosted Software Release. PowerPlan will deploy these changes to Client's PowerPlan-hosted production environment based on a published schedule.

Authentication Requirements:

To help ensure the security of the Hosted Software and Platform, PowerPlan requires that the Hosted Software be integrated with Client's identity provider (IdP) for authentication. This provides better security controls to ensure that user access is revoked immediately upon termination as a part of the client's normal HR and IT offboarding processes. Additionally, PowerPlan recommends that Client implement multi-factor authentication (MFA) for authenticating to Client's network/IdP. Implementing both MFA and integrating with Client's IdP will help provide significant security benefits and will reduce the risk of a security breach.

PowerPlan Hosted Software Authentication Integration Requirements. The following Hosted Software modules integrate using LDAP: Mobile Approvals, Asset Decision Support, Asset Investment Planning, and Visual Leveler. All other Hosted Software modules integrate using SAML 2.0.

Audits:

1. PowerPlan will conduct SOC 1 Type II and SOC 2 Type II audits of its cloud hosting operations no less often than annually. The SOC 1 Type II and SOC 2 Type II reports will be available within ninety (90) days of the end of the applicable audit period. PowerPlan will provide the latest available reports to you upon written request.
2. For SOC 1 (SSAE18) purposes, in the event the last available SOC 1 Type II report does not cover your requested time period, PowerPlan will, upon written request, provide a letter which will include details of any major changes to controls since the last audit period, if applicable.
3. Clients do not have the right to conduct an independent audit or review of PowerPlan's policies, procedures, or facilities (including Data Centers). However, subject to PowerPlan's confidentiality obligation or limitations on disclosures in accordance with industry best practices and the advice of its security advisors and auditors, PowerPlan will work in good faith to provide reasonable information regarding its policies and procedures upon receiving your written request for the same. For the avoidance of doubt, any information provided pursuant to this Audit section must be kept strictly confidential and solely used for Client's internal purposes.

Plans:

1. PowerPlan will maintain a Cybersecurity Incident Response Plan, which is designed in accordance with ISO 27001 standards and will be reviewed and tested no less frequently than annually.
2. PowerPlan will maintain a Disaster Recovery Plan, which is designed in accordance with ISO 27001 standards and will be reviewed no less frequently than annually.

Notice:

In the event of a breach of your Hosted Data, PowerPlan will notify your Authorized Application Administrator(s), based on the contact information last provided to PowerPlan, of the event within seventy-two (72) hours of validation. Such notice will include known details about incident, subject to confidentiality obligations and applicable laws. Except as required by law, PowerPlan will not publicly announce a breach of your Hosted Data, although it may announce it has suffered a security breach generally as it reasonably determines to be necessary.

SAAS, CLOUD SERVICES, AND SUBSCRIPTION SERVICES DO NOT INCLUDE ANY CLIENT SECURITY REQUIREMENTS BEYOND THOSE SET FORTH IN THIS SECURITY POLICY AND POWERPLAN DOES NOT MAKE ANY OTHER REPRESENTATIONS OR CERTIFICATIONS REGARDING ITS OBLIGATIONS AS THEY RELATE TO THE HOSTED DATA.