INFORMATION SECURITY OVERVIEW

Trust Center Overview

Dividend Portfolio Planner

Document control	Value
Policy owner	Dividend Portfolio Planner
Approved by	Not Applicable - Public Overview
Effective date	September 3, 2026
Version	1.0
Review cycle	At least annually and after material security, legal, product, or infrastructure changes
Classification	Public

Document objective: Provide customers, prospective customers, partners, and other stakeholders with a clear public overview of the safeguards Dividend Portfolio Planner (DPP) uses to protect information and support secure, reliable operations.

Publication note: This document is intended for the DPP Trust Center. It summarizes security practices without disclosing confidential architecture, internal procedures, vulnerability details, credentials, personal information, or other sensitive operational information.

1. Purpose

Dividend Portfolio Planner (DPP) recognizes that protecting customer information and maintaining the security and availability of the Platform are essential to user trust. This Information Security Overview describes DPP's externally facing security commitments and the principal safeguards used to protect the confidentiality, integrity, and availability of information.

DPP maintains an information security program designed around risk-based security management, least-privilege access, defense in depth, secure-by-design development, privacy-by-design, security monitoring, incident response, business continuity, and continuous improvement.

2. Security governance

DPP maintains an information security governance framework that assigns responsibility for identifying, evaluating, managing, and monitoring information security risks. Security responsibilities are incorporated into technology operations, software development, access management, vendor oversight, data protection, and incident management.

The security program is reviewed periodically and updated to address material changes in Platform functionality, technology infrastructure, threats, vendors, data-processing activities, and applicable legal or contractual requirements.

3. Risk management

DPP uses a risk-based approach to information security. Potential risks to DPP systems, information, users, and operations are evaluated based on likelihood, potential impact, existing safeguards, and business significance.

Security risks may be evaluated when new technologies or services are introduced, Platform functionality materially changes, new third-party providers are engaged, significant vulnerabilities are identified, security incidents occur, or relevant threat conditions change. Identified risks are addressed through appropriate mitigation, avoidance, transfer, or formal risk-acceptance processes.

4. Data protection

DPP applies safeguards based on the sensitivity and intended use of information. Customer account information, portfolio information, subscription information, and other nonpublic customer information receive protections appropriate to their sensitivity.

1. Encryption of information in transit and, where appropriate, at rest.
2. Role-based and least-privilege access restrictions.
3. Data minimization and controlled sharing.
4. Retention controls and secure deletion practices.

5. Identity and access management

DPP maintains access controls designed to ensure that access to systems and nonpublic information is limited to authorized individuals and services with a legitimate business need.

5. Unique identities and attributable access.
6. Least-privilege and need-to-know access.
7. Role-based authorization.
8. Multifactor authentication for privileged access.
9. Periodic access reviews and prompt removal of unnecessary access.

6. Authentication and credential protection

DPP maintains safeguards designed to protect account credentials and authentication mechanisms. Credentials, authentication secrets, security tokens, recovery information, and other sensitive authentication information are subject to access and handling restrictions.

DPP may use multifactor authentication, session controls, access monitoring, and other security mechanisms based on account type and risk.

7. Platform and infrastructure security

DPP applies security practices to the systems and infrastructure supporting the Platform. Production environments are managed separately from development and testing environments where appropriate, and DPP seeks to minimize unnecessary exposure of administrative interfaces, databases, systems, and sensitive services.

10. Secure system configuration and access restrictions.
11. Encryption and environment separation.
12. Security patching and vulnerability management.
13. Security logging, backup protection, and change management.

8. Secure software development

Security and privacy considerations are incorporated into DPP's software development and change-management processes. Depending on the nature and risk of a change, activities may include security and privacy requirements during design, authentication and authorization review, code review, dependency and vulnerability scanning, secret detection, automated testing, change approval, deployment controls, and post-deployment monitoring.

DPP maintains controls intended to prevent sensitive production credentials and restricted information from being unnecessarily incorporated into software source code or development materials.

9. Vulnerability management

DPP maintains processes designed to identify, assess, prioritize, and remediate security vulnerabilities affecting the Platform. Findings are evaluated based on factors such as severity, exploitability, exposure, system criticality, potential customer impact, and potential data impact. Material findings are tracked through remediation and validation.

10. Security monitoring

DPP maintains logging and monitoring capabilities designed to identify security events and unusual activity affecting important systems. Security events are evaluated and escalated based on their potential impact.

14. Authentication and administrative activity.
15. Account and permission changes.
16. Application and configuration changes.
17. Authorization failures and security-control failures.
18. Other potentially suspicious or anomalous activity.

11. Incident response

DPP maintains procedures for identifying, investigating, containing, remediating, and recovering from information security incidents. Where notification to affected parties or regulatory authorities is required by applicable law, DPP evaluates and addresses those obligations as part of its incident-management process.

Identify and evaluate the event.
Contain affected accounts, systems, or services.
Investigate potential impact.
Correct identified vulnerabilities or configuration issues.
Restore affected services and increase monitoring where appropriate.
Evaluate applicable notification requirements.
Document lessons learned and corrective actions.

12. Business continuity and recovery

DPP maintains business continuity, backup, and recovery practices designed to support restoration of important Platform services and information following an interruption. Recovery capabilities are periodically evaluated to identify potential gaps and opportunities for improvement.

13. Third-party security

DPP uses third-party technology and service providers to support certain Platform operations. DPP evaluates third-party security and privacy considerations based on the nature of the service, information involved, access provided, and potential business impact.

Where appropriate, third-party oversight addresses security safeguards, confidentiality, access controls, data protection, incident notification, data retention, secure deletion, and termination of access when services end.

14. Payment information

DPP seeks to minimize its exposure to payment-card information. Payment processing is designed to use an appropriate third-party payment service rather than requiring DPP to maintain full payment-card numbers or card security codes within DPP systems. Access to payment-related information maintained by DPP is restricted according to business need.

15. Customer privacy

Information security and privacy are complementary components of DPP's data-protection program. DPP seeks to collect information for legitimate and disclosed purposes, limit collection to information reasonably necessary to provide and protect the Services, restrict access to nonpublic information, maintain appropriate retention practices, support applicable customer privacy rights, and securely delete or de-identify information when appropriate.

For additional information, users should review DPP's Data Privacy, Retention and Deletion Policy available through the DPP Trust Center.

16. Security awareness

Individuals with authorized access to DPP systems or information are expected to follow applicable security requirements. DPP maintains security and privacy awareness practices designed to reinforce responsibilities relating to credential protection, account security, social-engineering risks, handling of customer information, secure use of technology, incident reporting, and protection of nonpublic information.

17. Continuous improvement

Information security is an ongoing process. DPP periodically evaluates its security program using information obtained from risk assessments, vulnerability management, security monitoring, access reviews, incident analysis, recovery testing, vendor reviews, Platform changes, and security-control assessments. Findings are evaluated and used to improve safeguards where appropriate.

18. Shared security responsibility

Protecting information also requires responsible actions by Platform users. DPP encourages users to maintain strong and unique passwords, protect account credentials, use available security features, maintain control of devices used to access DPP, review account activity when appropriate, and promptly report suspected unauthorized account activity.

19. Related Trust Center documents

Document	Purpose
Information Security Overview	Provides a public overview of DPP's information security program and safeguards.
Access Control Policy	Describes DPP's approach to authorization, authentication, access management, and access review.
Data Privacy, Retention and Deletion Policy	Describes DPP's approach to privacy, data retention, customer privacy requests, and secure deletion.
Terms & Conditions of Use	Establishes the terms governing customer use of the DPP Platform, including educational-use and investment-risk disclosures.

20. Security questions and reporting

Questions regarding DPP's information security or privacy practices may be submitted through the official contact methods published on the Dividend Portfolio Planner website or Trust Center. Potential security vulnerabilities or suspected security incidents should be reported using DPP's designated security or support reporting channel.

For security reasons, DPP does not publicly disclose information that could reasonably increase the risk of unauthorized access, circumvention of security controls, or compromise of DPP systems or customer information.

21. Document review

This Information Security Overview is reviewed at least annually and may be updated as DPP's technology, services, security program, or applicable requirements evolve. DPP may update this document without disclosing confidential security architecture, security configurations, internal procedures, testing results, vulnerabilities, credentials, personnel information, or other information that could increase security risk.

Trust Center Notice

This Information Security Overview is intended to provide customers, prospective customers, business partners, and other interested parties with a general description of Dividend Portfolio Planner's information security practices. It does not disclose confidential security configurations, system architecture, internal security procedures, vulnerabilities, security testing results, credentials, personal information, or other sensitive operational information. The controls described in this document may evolve as DPP's Platform, technology, risk environment, and security program develop.