shortpoint

ShortPoint SPFx

Security Information.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

GDPR

SOC 2

SOC 3

shortpoint

ShortPoint SPFx Security Information

ENVIRONMENT AND VERSION

This guide is for Microsoft 365 and SharePoint 2019 users.

TRUSTED BY:

SAMSUNG, Peace Corps, pwc, University of Michigan, Marathon, xfinity, Mitsubishi Heavy Industries, Ltd., Knoll, NASA, Volkswagen

Version **1.4**

Magdalene Mojica
Jan 06, 2026

security@shortpoint.com

shortpoint

Table of Contents.

Intro

We Think Security

Intranets are incredible tools that help teams collaborate and share information seamlessly within organizations. Modern platforms like Microsoft 365, SharePoint, and Microsoft Teams have revolutionized workplace productivity. Of course, with all that valuable information online, security is naturally top of mind.

At ShortPoint, we completely understand your concerns about keeping your intranet safe and secure. Security is woven into the fabric of everything we build.

This guide will walk you through exactly how we've designed ShortPoint to enhance your SharePoint environment without ever touching your data. You'll discover how the information you create, store, and share stays entirely within your own environment. We'll also share the robust security practices we follow internally to keep our operations protected from unauthorized access and other threats.

Section 1

How ShortPoint Protects Your Data

*"At ShortPoint, securing data is more than just a feature; it's at the heart of everything we do. From our dedicated team to the processes we follow and the innovative technology we develop, security remains our top priority. We embrace a "**Security by Design**" philosophy, meaning we prioritize protecting data right from the start, not as an afterthought."*

Your Data Stays in Your Space

Here's the most important thing you need to know about ShortPoint's security: ***your content always stays within your SharePoint environment***.

When you install ShortPoint, it operates entirely inside your own SharePoint Online system. To put it simply, think of it like installing an app on your phone. It uses your data, but the data stays on your phone. ShortPoint works the same way with your SharePoint sites.

We built ShortPoint on Microsoft's SharePoint Framework. It is designed to maintain the highest level of security by ensuring it never accesses, modifies, or stores your content. This means that your sensitive data remains fully protected.

How ShortPoint Actually Works In SharePoint Servers

When you use a ShortPoint Design Element on your page, here's what happens behind the scenes in your SharePoint Online environment:

ShortPoint works directly with SharePoint security features. This means that we don't create any new pages or complicated structures. For example, when you add a Design Element to your SharePoint sites, ShortPoint simply saves some plain text code. This code serves as a set of instructions that the ShortPoint engine reads to display the beautiful Design Element you added. As a result, when someone views your page, they can see the amazing designs you've created.

ShortPoint is fully compliant with Microsoft 365 and SharePoint security best practices. It uses SharePoint Client Side and REST APIs to make calls to existing site content. Because it uses SharePoint's built-in security features and site permissions system, all your existing security settings automatically apply. Think of it like this: if someone doesn't have user permissions to see something in SharePoint, they won't see it through ShortPoint either.

Here is what you can expect after you install ShortPoint SPFx into Office 365:

1. The app will appear in the list of installed apps in the Tenant App Catalog.

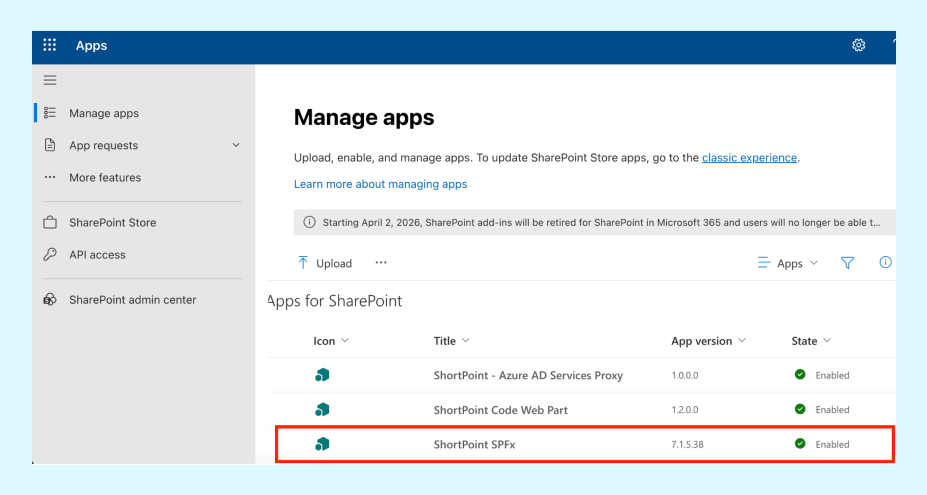

Figure 1.1 App Catalog

2. Two new items will appear in the Site Contents of the site where you installed ShortPoint:
    - ShortPoint SPFx
    - ShortPoint SPFx Dashboard

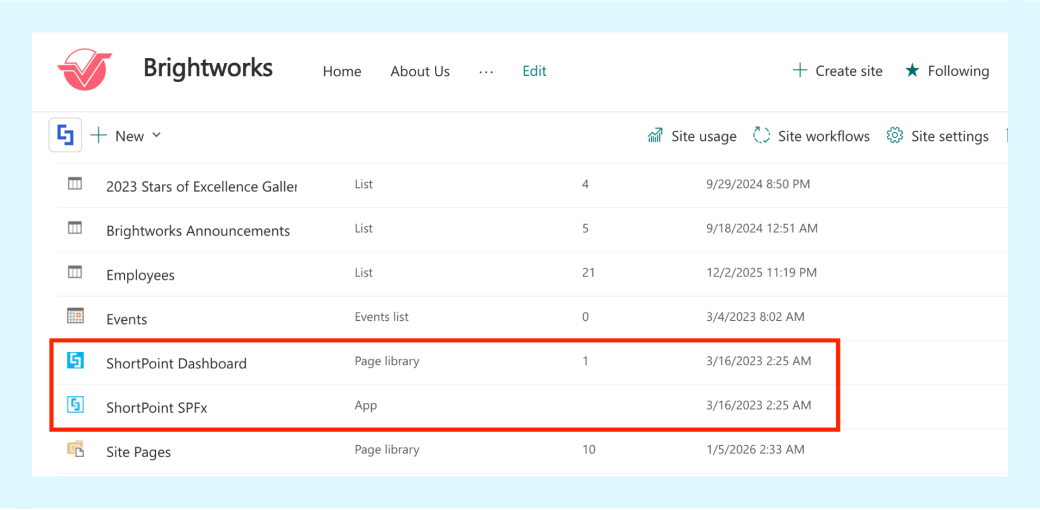

Figure 1.2 ShortPoint Dashboard & ShortPoint SPFx

These new items will not appear on other sites except the one where the initial installation of ShortPoint was made until you decide to add ShortPoint to more sites.

3. The ShortPoint web part icon will become available in the list of available web parts that you can add while editing a Modern SharePoint Site Page.

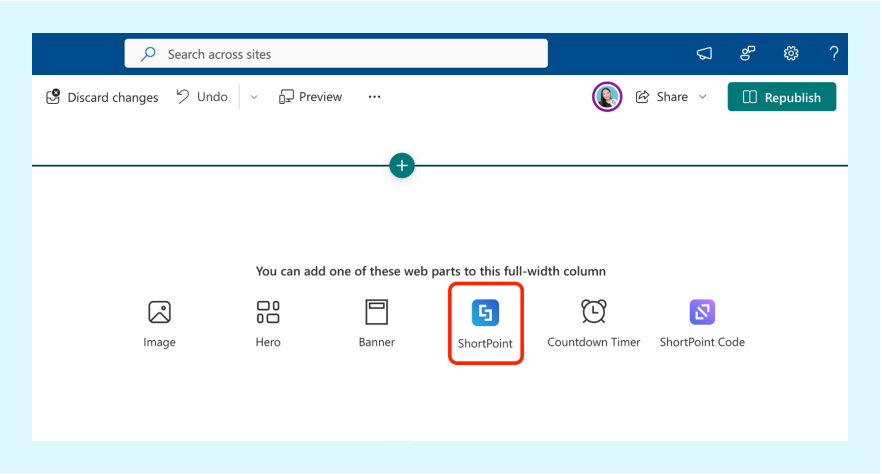

Figure 1.3 ShortPoint web part

4. If you use Classic SharePoint Pages and you selected to install ShortPoint on Classic Pages, you will have two Plus icons appearing in edit mode in the toolbar of the page.

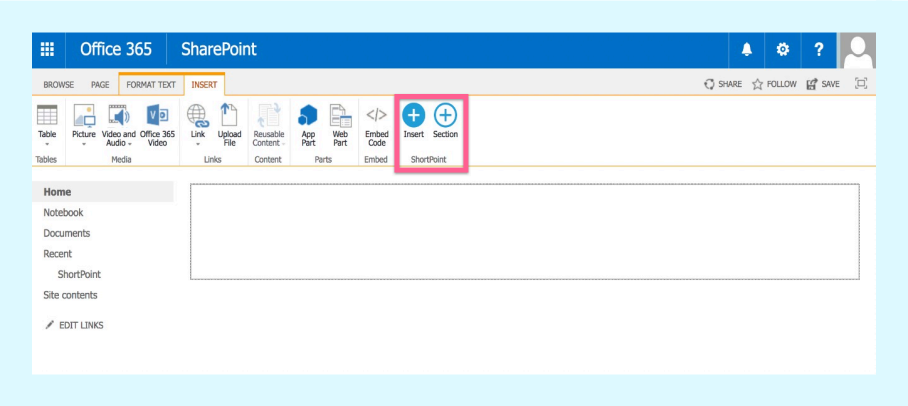

Figure 1.4 Insert buttons in Classic Pages

Other than these changes, there will be nothing else that appears in your environment after installing ShortPoint SPFx.

No existing page designs will be affected. ShortPoint will not change lists, libraries, system, or content pages in your environment, nor will it affect the existing look and feel (branding) of your Intranet after installation.

Section 2

What Data Is Collected

"At ShortPoint, your data stays within your environment. ShortPoint does not access, store, or process customer content or data from your SharePoint environment."

ShortPoint does not access, store, or process customer content or data from your SharePoint environment. ShortPoint only collects the following:

ShortPoint License Activation and Protection Information

Below is the information needed for License Activation:

- First Name
- Last Name
- Business Email
- Direct Phone
- Country
- Job Title
- Company Name
- Company Type
- Environment
- Tenant URL
- Number of ShortPoint Editors

Product usage statistics to understand how ShortPoint App is being used

Product usage stats are used to feed you our roadmap and provide you with better customer support. ShortPoint only sends the counters' data on how many times you used a particular ShortPoint feature. ShortPoint does NOT collect or store any site pages or content.

Below is the usage information collected by the ShortPoint App:

- ShortPoint Users Information (email, name, and all available profile properties);
- ShortPoint License information used for the activation
- Browser information for debugging and support
- Counters' data on how many times the ShortPoint User:
    - Opened the Page Builder
    - Inserted the ShortPoint Design Element and what that Design Element was
    - Opened the Theme Builder
    - Used the Power BI
    - Installed ShortPoint, and the site URL where it was installed
    - Uninstalled ShortPoint, and the site URL where it was uninstalled
- Current page URL
- Environment ID and type (Microsoft 365, SharePoint 2019, SharePoint 2016, SharePoint 2013);
- ShortPoint version;
- ShortPoint package type (WSP Solution, Add-in, SPFx);

Below is the usage information collected by the ShortPoint App for Page Viewers of sites built using ShortPoint:

The following anonymized properties are collected solely for the purpose of tracking page views on sites constructed with ShortPoint, to help provide better support and improve user experience by exclusively monitoring and analyzing the usage of ShortPoint features on the respective sites, ensuring optimal performance and user satisfaction:

- Anonymized Unique User ID
- Anonymized Tenant ID
- Anonymized Page ID
- Anonymized Site ID
- ShortPoint Web Part added (true or false)
- ShortPoint Theme Builder in use (true or false)
- Environment Type (Microsoft 365, SharePoint 2019)
- Page Type (Classic or Modern)
- Site Type (Root or Subsite)
- ShortPoint Version

For all of the “Anonymized” values above. We will only receive a string of random letters and numbers that’s unique for each tenant/user/page/site, and that’s impossible to deanonymize.

For example, for mytenant.sharepoint.com we’ll get an anonymized value like “tenant-oajd2fa423awf64”. We can’t go back to mytenant.sharepoint.com from the anonymized value that we log.

ShortPoint keeps your data for at least three years. However, we respect your privacy, and you can request that we delete all your data from our systems at any time. Please send this request to **privacy@shortpoint.com**.

You can also check our complete information on privacy in our Privacy Policy.

Request Policy

Section 3

How ShortPoint Complies with GDPR

"We're committed to keeping the limited personal data we collect (license and usage information) safe, in accordance with the General Data Protection Regulation (GDPR)."

What Is GDPR?

General Data Protection Regulation, or simply GDPR, is a comprehensive privacy law that came into effect on May 25, 2018, across the European Union. Think of it like a rulebook that tells data controllers and organizations how they must handle your personal information. While it's a European law, its impact reaches far beyond Europe's borders, affecting any company that deals with EU residents' data, including data processors and those involved in international organisations.

The main goal of GDPR is simple: **to give you more control over your personal data and to make sure organizations handle it responsibly by implementing effective measures and respecting your fundamental rights**.

ShortPoint and GDPR Compliance

Transparency and data security matter to us. This is exactly why we ensure GDPR compliance at all times. Here's how we do it:

Assigning a Data Protection Officer

To make sure your personal data protection stays strong, we've designated specific people to serve both as our GDPR lead and Data Protection Officer (DPO). They serve as your privacy advocates within our business practices. They're here to ensure we're meeting our data protection obligations and legal compliance when it comes to your information.

Collecting Only What is Needed

Here's the good news: we keep data collection to a minimum. We only gather data that is necessary to activate your ShortPoint license and help you when you need support. For a detailed list of what is collected, refer to Section 2 of this guide.

Here's something important: we don't touch your actual content. Nothing you create in SharePoint or Microsoft 365 gets sent to us or stored on our servers. That stays entirely in your environment, under your control.

Keeping Your Data Only For a Specified Period

We don't keep your information forever. We hold onto it only as long as necessary. Depending on regulatory requirements and legal frameworks, this typically takes three to seven years. After that, we securely delete it using technical and organizational measures to ensure data security.

Following Strict Security Policies

Security isn't just a buzzword for us. We have clear procedures in place for handling the limited personal data we collect (license and usage information) and for managing any internal security incidents. Since ShortPoint does not store or process customer SharePoint content, no customer content is ever involved in these processes.

You're in Control of Your Data

At ShortPoint, you can rest assured that you have complete control over your data. Here's what you can do to exercise your rights according to GDPR:

Access, Fix, or Download Your Data

Want to see what information we have about you? Need to correct something that's wrong? Just reach out to us at privacy@shortpoint.com. You can also request your personal data in a format that's easy to read and transfer to another service if you'd like.

Delete Your Data

You have the right to ask us to delete your information at any time. Simply email privacy@shortpoint.com, and we'll remove your data from our systems in such a way that ensures data security and respects your user privacy.

Object to Processing or Request Restrictions

If you're not comfortable with how we're processing your data, you can ask us to just store your data without actively using it.

You can also stop product usage data collection by blocking access to the activation.shortpoint.com domain. Just remember that blocking this domain means some features won't work, including automatic license updates and user assignments. Certain Design Elements and Connections (like Teams, Power Apps, Power BI, and Outlook events) may also not function properly. It's a trade-off between privacy safeguards and functionality, and the choice is yours.

Section 4

How ShortPoint is Committed to Validating its Security Measures

"Security is at the heart of ShortPoint's operations, from our team members to our daily processes and the technology we use. And we don't just say that. We've constantly proven it."

SOC Reports: Independent Verification You Can Trust

SOC, which stands for Service Organization Control, isn't really as complicated as it sounds. Think of it like a health checkup for security. **SOC reports are created by independent auditors, specifically Certified Public Accountants,** who examine how well a company manages and protects its internal systems and security controls that support the product.

These auditors conduct a thorough risk assessment and gap analysis focusing on the organization's internal controls to safeguard customer data. They look at five key areas called the **five Trust Services Criteria**, created by the American Institute of Certified Public Accountants (AICPA):

- **Security** - this criterion is all about protecting systems from unwanted guests. This covers everything from access controls to how the company monitors for threats and to what happens if something goes wrong. These security practices are essential for maintaining a strong security posture and effective risk mitigation.
- **Availability** - ensures the system is up and running when you need it. Nobody likes a service that's constantly down, right? This looks at uptime, backup systems, disaster recovery plans, and adherence to service level agreements (SLAs), which are critical for maintaining trust with customers and partners.

- **Processing Integrity** - ensures a company's internal systems operate consistently and reliably as designed.
- **Confidentiality** - is basically about keeping secrets secret. It examines how companies protect information they've designated as confidential throughout their entire life. From when they first collect it to when they eventually delete it, the data should be protected. This is especially important for cloud service providers and managed service providers who handle sensitive client information.
- **Privacy** - takes things a step further by looking at personal information specifically. It ensures companies are handling your personal data according to their privacy policies and following privacy controls and best practices.

These key areas are the gold standards for keeping data safe. Using these criteria, auditors develop detailed reports, specifically SOC 2 Type II and SOC 3. To help you better understand each one, here's what they mean:

SOC 2 Type II

SOC 2 Type II examines the design and operating effectiveness of a company's security controls. It ensures that they are working effectively over an extended period, usually at least three months. This high level of scrutiny provides stronger assurance to user entities and business partners that the service organization's controls meet the highest standards for secure operations and governance.

The process is thorough but straightforward. An independent auditor with an understanding of the auditing framework comes in to understand how the company's systems and processes work within the defined audit scope. Then, over the examination period, they test everything to make sure it's actually working as

claimed. They'll review security questionnaires, examine documentation, talk to employees, watch processes in action, and run technical tests on security systems.

The result is a detailed SOC 2 audit report that shows what necessary controls are in place, what tests the auditor ran, and whether everything passed muster. This report is detailed and technical. It includes everything you need to know about an organization's security controls.

SOC 3

While SOC 2 Type II reports are incredibly detailed and contain sensitive information that companies typically don't want to share publicly, sometimes you need a report that demonstrates your organization's ability to protect customer data in a way that can be shared widely. That's exactly where SOC 3 comes in.

A SOC 3 examination involves the same rigorous testing as SOC 2 Type II and uses the same AICPA's Trust Services Criteria. The key difference lies in how the results are reported. Instead of a lengthy, technical official audit document, SOC 3 produces a streamlined and summarized report that can be shared with anyone, including posting it publicly on websites or in marketing materials.

ShortPoint Achieve SOC Compliance

Recently, ShortPoint completed SOC compliance audits. The SOC examination specifically covered our application and controls relevant to the Trust Service Criteria for security. The independent service auditor concluded that our security controls were suitably designed and operated effectively. These reports prove our service commitment to you.

And to ensure that we keep it that way and remain compliant, **ShortPoint uses real-time automation for the continuous monitoring of our internal security controls**. These automated processes ensure ongoing alignment with industry-leading practices and evolving compliance requirements. You can request the report by clicking the button below.

Request Report

Section 5

How ShortPoint Keeps the Development Lifecycle Safe and Secure

"ShortPoint thinks and breathes security. It is woven into everything we do, even the development process."

Built-In Software Security Right From the Start

It is important to note that all references to data or content in this section refer only to ShortPoint's own internal corporate data and not customer SharePoint content.

We carefully follow a secure software development lifecycle (SSDLC) process that ensures our software is not only reliable but also meets the highest security requirements. Even from the start, security is at the forefront. It is integrated into every stage of our development process.

Planning and Design Phase

Before we write a single line of code, our software development team focuses on security requirements. We identify potential security risks and vulnerabilities. At the same time, we figure out what security controls need to be in place. We ask questions like: What sensitive information will this handle? Who needs access to it? What could go wrong, and how do we prevent it?

Development and Testing Phase

As we develop our software, we continuously test it to catch any security issues and ensure software security. Every feature gets thoroughly checked before moving forward with automated tools and code reviews. We also use automated static analysis and code-quality checks to help identify potential issues early in the development cycle. These tools enforce our internal secure coding standards and prevent common vulnerabilities before the code is reviewed by the team.

Our Team's Commitment to Secure Coding Standards

ShortPoint believes that our processes are only as strong as our team. So, we invest heavily in making sure that our developers have the knowledge and skills to write secure code. They are trained to follow the latest secure coding guidelines and security frameworks.

Training That Matters

All our developers receive specialized training in secure coding practices and security awareness. They also get extra training on how to defend against online threats and prevent security breaches. This ongoing education ensures our application development teams are well-equipped to handle evolving threats and stay up to date with techniques essential for developing secure software.

The Four-Eyes Principle

Here's a simple but powerful rule: no one reviews their own work. Every piece of code undergoes code reviews by at least one other developer who understands security concerns and knows what to look for. This extra set of eyes helps catch security flaws and mistakes early, ensuring higher software integrity and quality before anything goes live.

How We Handle Changes Safely

Even small software changes can have big impacts on the overall software development cycle and the security posture of the product. That's why we have a structured Change Management procedure for any modification, no matter how minor. This process ensures the proper documentation, testing, and approval of any change migrating to the production environment.

Before Any Change Happens

- Someone with authority must approve the proposed change.
- The change gets documented, so there's a clear record.
- Only authorized team members can submit changes.

Continuous Testing

Every change goes through rigorous security testing on systems completely separate from what our customers use. We check that it works properly, doesn't break anything else, and, most importantly, doesn't create any security vulnerabilities.

Final Review and Approval

Before a change goes live, it needs a final sign-off from management. No one can deploy a change without approval. And, if something unexpected happens, we also have a backup plan ready. We can quickly roll back to the previous version in case anything goes wrong.

Keeping Production Environments Protected

ShortPoint implements strong segregation of duties. This simply means that we maintain strict boundaries between where we develop the software and who deploys the change.

Separate Spaces

Our development, testing, and production environments are kept separate. This means experimental work never accidentally affects live systems that customers are using, reducing the risk of security vulnerabilities during the deployment phase.

Controlled Access

By design, developers can't just push changes directly to production. Only specially authorized personnel with elevated access can deploy to the live environment. This checkpoint ensures that everything going to production has been properly vetted through security reviews and approval.

Section 6

How ShortPoint Ensures Business Continuity

"We're committed to protecting the limited operational data we collect (licensing and usage information) and maintaining normal operations through careful risk assessment, detailed planning, regular testing, and proactive preparation."

Our Blueprint: Clear Plans for Any Situation

It is important to note that all references to "data," "backups," or "information recovery" in this section refer only to ShortPoint's own internal corporate systems, not customer SharePoint data.

Think of business continuity planning like having a well-rehearsed emergency plan; you hope you'll never need it, but you're prepared if you do. ShortPoint maintains two key plans as part of its business continuity management systems:

Our Security BluePrint

Business Continuity Plan

Disaster Recover Plan

Business Continuity Plan (BCP)

This is our comprehensive roadmap for maintaining critical business functions and operations during any business disruption. It outlines exactly how we'll respond to unexpected events and keep serving you without missing a beat, ensuring we can resume normal operations as quickly as possible.

Disaster Recovery Plan (DRP)

This plan kicks into gear during other major business disruptions or emergencies. It prioritizes which business systems and critical services need attention first and maps out step-by-step recovery operations to minimize data loss and downtime.

System Categorization

To make smart decisions about priorities, we perform a Business Impact Analysis (BIA). To put it simply, we analyze how each system affects our ability to serve you. Then, we make plans accordingly based on the analysis. This structured approach ensures that recovery efforts focus on minimizing impact and maintaining mission continuity. We organize our systems into two categories:

Mission-critical systems

These are the systems that support ShortPoint's internal operations, licensing, support, and availability. They need immediate attention because they handle data directly.

Non-critical systems

Systems that are not categorized as critical are placed here. When a threat occurs, these systems can wait a bit longer.

Regular Testing of Business Continuity Strategies

We believe that having plans on paper isn't enough. We put them to the test at least once a year through realistic simulations. Here's how we ensure our business continuity plans are tested regularly and are effective:

Tabletop Exercises

Our key team members gather to walk through emergency scenarios step-by-step. This training ensures everyone understands their responsibilities and can respond quickly when a crisis occurs.

Technical Testing

We practice switching to backup systems and alternate locations. This includes restoring information from data backups and verifying that all communication channels work properly. We don't just assume our backups will work; we prove it.

After each test, we document the potential impact. We note what went well and what needs improvement, then update our plans accordingly. This ongoing cycle of learning helps us develop strategies to protect our service and maintain organizational resilience through any disaster, outage, or cyber attack.

Crisis Management

One of our top priorities is to ensure that ShortPoint's internal operational systems remain available so your ShortPoint product experience is not disrupted. Here's how we make that happen:

Smart Backup

We use cloud infrastructure with a smart backup strategy. ShortPoint's internal systems and operational data are backed up across multiple secure locations. If one system has issues, another seamlessly takes over, minimizing downtime and supporting critical business functions. All backups are encrypted for security, and only authorized key personnel can access them, safeguarding sensitive information and meeting the expectations of key stakeholders.

Effective Communication

We're also big believers in transparency. If something does go wrong, you'll see real-time updates on our status page. You won't ever have to wonder what's happening or when things will be back to normal. Behind the scenes, automated monitoring systems keep watch 24/7. If something looks off, our dedicated team gets notified immediately so we can jump into action and get things back on track fast.

Section 7

How ShortPoint Classifies & Encrypts Internal Data

"We believe that keeping data secure isn't just about having the right technology. It's also about maintaining trust through consistent, reliable security practices that work together to safeguard what matters most to you and your business."

Our Security Approach

It is important to note that **ShortPoint does not access, store, or process customer content or data from your SharePoint environment**. The data classification, encryption, and retention practices described in this section refer only to ShortPoint's own internal corporate data and not customer SharePoint content.

Our security approach is built on three key principles: **understanding the data, ensuring it stays safe, and making sure it's kept for the right amount of time**. We continuously monitor our systems and review our security settings every year to make sure we're meeting the highest standards. Independent experts regularly assess our security

measures to verify they're working as intended. The controls we have implemented have been independently assessed for design and operating effectiveness.

Understanding Your Data: How We Classify Information

Understanding and classifying the kind of data we have helps us determine the right level of protection for each type. This allows us to apply the appropriate access control and user permissions. No single ShortPoint employee has full control of your data. Every data type can only be accessed by authorized users.

By managing security through careful classification and encryption, we prevent unauthorized sharing and data leaks, ensuring data integrity. Here's how we break it down:

Restricted/Confidential Data

This is classified as the most sensitive information. It's the type of data that could cause serious problems if it fell into the wrong hands. It might include highly sensitive data or business information about ShortPoint. Unauthorized disclosure, alteration, or destruction of confidential data could cause a serious or significant level of risk to ShortPoint or its customers.

We treat this data with the highest level of security. To protect it, we create explicit permissions guidelines, limiting access to only those specific employees who absolutely need it to do their jobs. We think of it like a vault with only a few trusted keyholders, ensuring access control and preventing unauthorized users from gaining access.

Internal Use Data

This category covers information that isn't necessarily secret, but shouldn't be publicly available either. Data is classified as Internal Use when its unauthorized compromise could result in a moderate level of risk to ShortPoint or its customers.

We assign permissions carefully to protect this data from unauthorized access. It is only shared with employees who have a legitimate business reason to see it. Any data that is not assigned as restricted or public is automatically treated as Internal Use data. By

applying strict access control and sharing settings, ShortPoint ensures compliance standards and prevents any data breaches.

Public Data

This is information that's already public or wouldn't cause harm if it became public. Data classified under this type results in little or no risk to the company or its customers. While we don't worry as much about keeping it confidential, **we still make sure it can't be tampered with or deleted without authorization by implementing strict access control and permissions**. Even if these types of content may have no potential risks, we are still committed to maintaining security and following security best practices.

Encryption: Data's Security Blanket

ShortPoint ensures that data is protected using appropriate cryptographic controls consistent with its security policies, classification requirements, and compliance standards. To put it simply, **we use super-strong encryption to protect sensitive information**. Whether it's stored within our systems or traveling across the internet, we keep data safe and protected.

The encryption process is like a security blanket for information. It blocks access to unauthorized users and ensures that only those with the right permissions have access to decrypt and open data. By implementing these security features, we help prevent unauthorized sharing and maintain the data integrity of content throughout its lifecycle.

When Data Is Stored (Data At Rest)

All production data stored on our systems is encrypted, no exceptions. This includes databases, file systems, and sensitive information. We manage the encryption keys ourselves and keep them under strict security controls, accessible only to specially authorized accounts. This robust encryption practice is a crucial part of securing and maintaining data integrity.

When Data Is Moving (Data In Transit)

Anytime data moves between systems, we use strong end-to-end encryption. This security measure applies to communications with cloud infrastructure and third-party vendors, and applications. This creates a secure tunnel that keeps your information safe from prying eyes and helps in preventing unauthorized sharing and data leaks.

We make sure that both internal and external communications are encrypted and authenticated by strong protocols, ensuring user authentication is robust and compliant with security settings. If we need to send particularly sensitive information through email or messaging, we require end-to-end encryption to be fully enabled first. Otherwise, transmission of restricted or sensitive data over electronic end-user messaging channels is prohibited, in line with our compliance standards and regulatory requirements.

Keeping Data for the Right Amount of Time

We follow a simple philosophy when it comes to data retention policies: **keep what we need, for as long as we need it, and no longer**. This approach is guided by three principles: fairness, necessity, and security. By implementing clear retention policies within our security framework, we ensure compliance with regulatory requirements. These policies help us limit access to sensitive data over time, reducing risk and supporting data integrity throughout the lifecycle of your information.

How Long Do We Keep Data

We only hold onto data as long as there's a legitimate reason to do so, adhering strictly to our security and data retention policies. This might be because:

- Legal regulations require it, ensuring compliance with regulatory requirements
- Our contract with you specifies it,
- It's necessary to provide the services you've requested.

For customer data, we follow the retention periods outlined in your product terms and service agreements. Throughout this time, we store your data in secure systems with full audit trails to ensure it stays protected, leveraging security features like access control and continuous monitoring.

What Happens When It's Time to Let Go

When data reaches the end of its retention period, we don't just hit delete and call it a day. **We have specific procedures to ensure information is destroyed securely and completely**, in line with our data loss prevention policies and compliance standards. These procedures include documented evidence of disposal actions, noting the date and method used, helping us maintain full audit trails and meet regulatory requirements.

- **For digital data**, we use secure wiping methods that make recovery impossible, supporting our commitment to securing content and protecting sensitive information.
- **Physical documents** are shredded to ensure they can't be reconstructed, following strict access control measures.
- **For physical assets** that store content or other critical data, we carefully review retention policies and properly wipe the drives according to best practices in data lifecycle management.
- And **when employees leave the company**, they return all company equipment. If they use personal devices for work, we ensure all business information is transferred to us and securely erased from their equipment. This process is part of our broader strategy to manage security and prevent users from unintentionally exposing sensitive data.

Section 8

How ShortPoint Keeps Internal Data Safe with Smart Security

"We believe that smart security isn't just about using the most advanced, complicated technology. Sometimes, it can be found in the simplest procedures."

Zero Trust Access

It is important to note that the data, content, and resources described in this section refer only to ShortPoint's own internal corporate data and not customer SharePoint content.

Our smart security approach is called "Zero Trust," which simply means we verify everyone before granting access to our systems. This strategy rests on two key ideas: giving people only the access they truly need for their jobs (or what we call the "least-access principle"), and using an extra layer of protection like multi-factor authentication when logging in. This keeps your information confidential, accurate, and available when you need it.

Least-Access Principle: Giving People Just the Right Amount of Access

Everyone at ShortPoint (full-time, part-time, contractors, or consultants) gets access to only what they need in order to do their jobs. Nothing more, nothing less. This approach helps us enforce permissions carefully, ensuring that users interact only with content relevant to their role, which is essential for maintaining strong security and protecting sensitive data.

How We Organize Access

ShortPoint applies a role-based access control (RBAC) system. It simply means that access to a system or any kind of information is based on job roles. Here's how it works:

- **Three Levels of Access**: We organize access into straightforward categories: Administrator (full control), User (standard access), and No Access. It's that simple.
- **Keeping Things Separate**: In our most important systems, we set things up so that no single person has control over everything. This prevents mistakes and keeps sensitive information extra secure.
- **Getting Permission**: Access is tied directly to what you do at work. If someone needs access to a system, they need to request it formally and get approval from their manager. If they need more than the basics, they'll need to explain why.
- **Special Access for Sensitive Areas**: Access to critical infrastructure is limited to authorized staff who have a clear business reason to be there.
- **Everyone Gets Their Own Login**: Each person has their own unique username and password. We don't allow shared accounts, and we disable default system accounts for security reasons.

Keeping Passwords Strong

Passwords tend to be overlooked when it comes to security. Probably because we're so used to creating one. But it's a different story here at ShortPoint. We know it's the first line of defense in protecting your data, so we take it very seriously. We drill into our employees how important it is to keep their passwords strong and teach them to apply these best practices:

- **Make Them Complex**: Whenever possible, passwords should be at least 10 characters long and include a mix of uppercase letters, lowercase letters, and symbols.
- **Keep Them Private**: Passwords are confidential. And all our team members know not to share them with anyone. We also ensure that passwords stored within systems are protected using strong, one-way hashing algorithms.

Double-Checking Your Identity with Multi-Factor Authentication

If you have an online account, you've probably heard of Multi-Factor Authentication (MFA). It's basically a security process where you log in with your password and then confirm your identity with a second method. For example, a code sent to your phone or a series of protected numbers sent to an authenticator app.

At ShortPoint, we also apply the same process. This extra step makes it much harder for unauthorized people, including external users, to gain access and helps protect your data from potential breaches. **Implementing MFA is a critical part of our conditional access policies designed to continuously monitor and secure user activity**, ensuring that only authorized users can access sensitive content and resources.

Here's our policy on MFA:

- **It's Required Everywhere Possible**: If a system offers MFA, we turn it on. No exceptions.

- **Essential for Remote and Sensitive Access**: To access our core production systems remotely, you must use MFA. This ensures only authorized personnel can get in, even from outside the office.
- **Secure Connections Only**: When connecting to our systems remotely, you need to use encrypted connections along with strong authentication.
- **All Remote Tools Protected**: Any tools we use to access company systems from other locations require multi-factor authentication.

Regularly Checking and Updating Access

Security isn't a "set it and forget it" thing. **We continuously review and update who has access to what, making sure everything stays aligned with our security principles and compliance requirements**. This ongoing process includes monitoring and managing explicit permissions and ensuring that security groups are properly configured to govern sensitive data and access effectively.

Regular Reviews

We periodically review system access to ensure it's still appropriate:

- **Checking Access Levels**: Management regularly reviews whether each person's access matches their current job responsibilities.
- **Making Corrections**: If we find that someone has more access than they need, we adjust it to meet our security standards.

Managing Access Over Time

Access changes as people's roles change:

- **Starting Out**: When employees join ShortPoint or take on a new role, they get access based on what that position requires.
- **Moving On**: When someone leaves the company or their contract ends, we remove their access within 24 hours. We also disable accounts that haven't been used in 30 days.
- **Staying Current**: Managers regularly review user privileges, and our administrators quickly remove access that's no longer needed.

Section 9

How ShortPoint Maintains Security with Continuous Defense

"From the people we hire to the processes we follow and the technology we use, protecting our systems, safeguarding the limited data we collect (license and usage information), and ensuring the security of the ShortPoint platform are our top priorities."

Continuous Defense Approach

It is important to note that all references to "data," "files," or "information" in this section refer only to ShortPoint's own internal corporate data and not customer SharePoint content.

The Continuous Defense approach is a comprehensive program that keeps us constantly watching, testing, and improving our security settings around the clock. Think of it as having a dedicated security team that never sleeps. It's always on the lookout for potential security risks and vulnerabilities before they become real issues.

Proactive Security: Continuous Detection of Weaknesses

Here in ShortPoint, we believe in the saying, "The best defense is to catch problems first; even before they actually become one." That's exactly why we're constantly checking our systems for vulnerabilities using advanced continuous monitoring and security features.

Round-the-Clock Vulnerability Scanning

We run continuous security scans, or what we call "Vulnerability Scans", across all our systems 24/7. This proactive approach ensures infrastructure security and protects data effectively. It allows us to spot new vulnerabilities or configuration issues as soon as they appear. This means that we see potential threats not weeks or months later, but right where we can prevent them from causing real problems.

We also deploy advanced security agents and tools on our employees' computers and other dedicated software. These tools automatically review our code for vulnerabilities to protect ShortPoint's internal systems and maintain a secure development process.

Regular Security Testing by Experts

Beyond automated scanning, we bring in real security experts to try to break into our systems (with permission, of course!). This penetration testing is done regularly (or even continuously) by either our certified in-house ShortPoint security professionals or independent third-party specialists who know all the tricks hackers might try.

We also build security features into our development process from day one. Every single code change goes through a mandatory security review by team members trained in secure coding practices. We use advanced protection techniques like code obfuscation to add extra layers of data encryption and security to our software. By tapping into all these, we enhance security and protect sensitive data.

Structured Remediation

We don't just identify security risks, we fix them fast. We believe that finding a security issue is only half the battle. What matters most is how quickly and effectively we address it. We consistently develop comprehensive Remediation plans that are strictly followed the moment an issue is identified.

Clear Timelines Based on Severity

When we discover a vulnerability, we immediately categorize it based on how serious it is and follow strict timelines for fixing it. We don't let critical issues sit around. They get immediate attention to maintain data security and protect sensitive files.

Here's how we prioritize:

- **Critical issues** - these are the most serious threats. It includes vulnerabilities that could impact internal systems, administrative access, or the limited personal data ShortPoint collects (such as license and usage information).
- **High-severity issues** - these are issues that could significantly compromise the security settings of our platform.
- **Moderate and Low issues** - these are issues that hold little to no risk.

While vulnerability priority levels guide the urgency of our response, we ensure to address all issues as swiftly as possible.

Mandatory Monitoring of System Activity

We have a Logging and Monitoring Policy that establishes comprehensive requirements for audit logging and monitoring of system activity across all ShortPoint system components.

What We Track

Our systems automatically create detailed records whenever important events occur, including key activities:

- Any attempts to access, change, or delete ShortPoint internal system data
- When people log in or out, and any failed login attempts
- Every action taken by administrators (since they have the most access)
- Changes to system settings, software updates, or security patches
- Any suspicious activity detected by our security tools

Protecting the Records Themselves

These logs are kept accurate using time synchronization based on official atomic time standards, ensuring precise tracking of all events. The logs themselves are protected from tampering through robust security measures and stored securely in backup servers separate from our main systems.

Real-Time Monitoring

We don't just collect logs and call it a day. Our systems actively monitor everything in real time. It immediately alerts us if something critical fails or looks suspicious. This proactive approach to continuous monitoring and enforcing security policies helps us quickly identify and respond to potential security incidents.

Incident Management and Response Plan

Prevention is always the key. But even with the best prevention, things can still go wrong. Good thing, ShortPoint is prepared for it. We have created a formal Incident Response Plan (IRP) to ensure quick and effective action when a breach happens. It involves identifying, containing, investigating, resolving, and communicating information related to the breach. And to ensure its effectiveness, we test the plan every single year.

Quick Reporting and Response

The whole ShortPoint team is trained to safeguard security. Each team member knows that if they see potential security incidents or risks, they are to report them immediately, no exceptions. When we see that our customers might get affected, we update our status page to keep you informed with transparency and timely communication.

Once we confirm that a security incident has occurred, we spring into action following our established incident response plan to contain the problem and stop it from spreading. We're careful to preserve all evidence during this process to enable a thorough investigation and support regulatory compliance requirements.

Recovery and Learning

After we've contained a security incident, we work diligently to recover any affected ShortPoint internal systems or operational data.

But we don't stop there. Once everything is back to normal, we conduct a thorough post-mortem review. We ask ourselves: What was the root cause? How can we improve our security settings? What can we learn from this to prevent future security incidents? This review process is crucial for enhancing our security best practices and reinforcing our continuous monitoring efforts.

If needed, we provide additional training to our team on enforcing security policies. We also incorporate these lessons into our ongoing security risk reviews and compliance obligations. By constantly developing our response plan, our security protocols grow stronger and more resilient.

Section 10

How ShortPoint Builds a Culture of Compliance

"We believe that protecting our customers' data and keeping our systems secure isn't just about technology; it's also about people."

Culture of Compliance

We understand that creating a company culture for security means fostering the people who monitor and administer it. The strength of our security measures depends on the dedication, awareness, and ethical standards of every person on our team. That's why we've built a **security-focused culture based on four key pillars: careful hiring practices, thorough security training with clear ethical standards, and transparent accountability**. Let's walk you through each pillar.

Starting A Good Security Culture: Our Hiring Process

Building a robust security culture begins with bringing the right people on board. **Before anyone joins the ShortPoint team, we conduct thorough background verification checks**. These checks are part of our standard hiring process and help us ensure that new team members are well-suited for their roles and aligned with our security best practices. We handle this screening responsibly, following all legal and ethical guidelines while matching the depth of our review to the sensitivity of the information each person will access. Independent auditors regularly review our screening practices to confirm they're working effectively and supporting our overall security program.

We also make sure that every new hire signs a confidentiality agreement on their first day. This reinforces our commitment to protecting sensitive information from

the start and emphasizes the importance of employee accountability in maintaining our organization's security culture.

Investing in Knowledge: Security Training Efforts

We make sure everyone at ShortPoint has the tools and knowledge they need to maintain our strong cybersecurity culture and uphold our security best practices.

Cybersecurity awareness training is essential for helping our team understand current security initiatives, recognize security risks, and appreciate the real-world impact of security incidents and data breaches. **Every new employee completes cybersecurity training during onboarding.** We also provide ongoing training programs to all team members throughout their time with us. These sessions cover security and privacy requirements, as well as secure practices for using company information and resources appropriately. This helps motivate employees to adopt good security habits.

Team members also review and acknowledge our Information Security policies, which explain the security expectations specific to their roles. This approach helps us foster a security-first company culture and reinforces the importance of every individual's role in maintaining the organizational culture of security.

Taking Responsibility: Accountability and Consequences

High standards only work when there's a clear system for ensuring everyone follows them. That's exactly why ShortPoint has a Code of Conduct. Here, we have spelled out our expectations for ethical behavior. **We expect every team member to be**

honest, act ethically, and demonstrate integrity in everything they do, while following all applicable laws, security policies, and security protocols.

When a team member gets hired, they are required to acknowledge our Code of Conduct. It includes clear policies about the consequences of non-compliance, reinforcing the importance of security practices and reporting security incidents promptly. We use a fair disciplinary process that provides structured corrective action and helps prevent repeated issues, particularly when someone is suspected of a security breach or engages in risky behavior. When determining the appropriate response to a violation, we consider relevant factors such as the person's training history, adherence to security protocols, and the severity of the offense.

Failing to follow our Code of Conduct or other security policies can result in disciplinary action, up to and including termination of employment. In cases of serious misconduct, we reserve the right to terminate employment immediately. This firm approach ensures that everyone understands their role in maintaining our security culture and the serious nature of violating security best practices.

Final Remarks.

You have now reached the end of this guide. Thank you for your interest in ShortPoint security.

If you need further assistance, you may reach out to us through the following methods:

- 🔐 Security Team Email - **security@shortpoint.com**
- 📩 Support Team Email - **support@shortpoint.com**
- 📚 Knowledge Base - **support.shortpoint.com**
- 🌐 Website - **shortpoint.com**

Elegant Intranet sites anyone can design.