

How Your Personal Information Is Used, Protected, and Securely Destroyed

We understand that submitting personal documentation such as dates of birth, social security numbers, marriage certificates, tax returns, and similar sensitive materials can raise questions about privacy and security. Protecting your information is a top priority for **Bolton**, and we want to be transparent about how your data is handled at every step.

1. How Your Personal Documents Are Transferred to the Platform

When you upload or provide documents as part of the audit or verification process, Bolton uses **industry approved, secure platforms** for transmitting confidential information. Bolton's Information Security Policy requires that **all confidential data transmitted externally must be encrypted using strong, industry standard encryption** to prevent interception or alteration during transfer.

Only authorized Bolton personnel are permitted to handle your documents, and access is strictly controlled, monitored, and limited to what is necessary to perform required audit functions. This aligns with Bolton's policies requiring **least-privilege access**, encryption during data transmission, and secure handling of all confidential data.

2. How Your Information Is Stored in bswift

The bswift platform is designed with a **comprehensive, risk-based security program** built on the **NIST 800 53 security framework**, a leading federal cybersecurity standard. According to bswift's published security materials, the platform maintains:

- Over **400 IT security controls**, reviewed and updated monthly
- Annual **SOC 1 Type 2** and **SOC 2 Type 2** assessments
- Hosting in a **SOC 2 certified data center**
- Participation in the Shared Assessments **SIG** program, covering more than 1,000 security, privacy, and resiliency controls

Additionally, bswift maintains business continuity and disaster recovery plans to ensure ongoing protection and availability of your data.

This means your personal information is stored in a highly controlled environment designed to protect data confidentiality, integrity, and availability at all times.

For more information, please review bswift's comprehensive security reporting webpage: <https://trust.bswift.com/controls>.

3. How Documents Are Destroyed After the Audit (and Timing of Destruction)

Bolton retains any physical documents you provide **in a secure onsite location**, accessible **only to authorized personnel** through **keycard-restricted private security zones**, in line with Bolton's physical security policies.

Once all documents have been securely provided to PWC and audit requirements are complete, **physical documents are securely destroyed** following Bolton's confidential data destruction protocols, which include methods such as **cross-cut shredding** to ensure information cannot be recovered.

Destruction occurs **after we receive PWC approval**, typically **6–12 months post audit**. This retention window supports compliance, quality assurance, and audit verification.

(Over)

In Summary

Your sensitive information is:

- ✓ **Transferred securely**

Using encryption and secure systems to prevent unauthorized access.

- ✓ **Stored within highly regulated, independently audited systems**

bswift follows NIST standards and undergoes rigorous SOC reviews annually.

- ✓ **Accessed only by authorized personnel**

In accordance with strict least privilege and access control policies.

- ✓ **Physically protected when held by Bolton**

Stored in keycard secured spaces until no longer required.

- ✓ **Destroyed using approved confidential data destruction methods**

Typically, 6–12 months after the audit, and only after approval from PWC.