

A decorative graphic consisting of two overlapping, curved shapes. The top shape is orange and the bottom shape is blue, both pointing towards the right. They are positioned above the main title text.

# Account Information Security

Merchant Guide



At Visa, protecting our cardholders is at the core of everything we do. One of the many reasons people trust our brand is that we make buying and selling safer and more secure. We also recognize that protecting cardholder information is critical to the business success of merchants around the world. That's why we make securing the payment system an ongoing priority. Our goal is to limit crime by making it more difficult to commit.

## VISA'S COMMITMENT TO CARDHOLDER PROTECTION

Growth in card usage has meant larger quantities of account information is processed and possibly stored by merchants and service providers. To protect the integrity of account information, all such entities must remain vigilant in safeguarding this sensitive data. Visa is committed to supporting financial institutions, merchants and their agents by ensuring that we all work together to help keep the payments system safe and reliable.

Visa has an ongoing commitment to protecting the integrity of *Visa*® account and transaction information. The Account Information Security Program, launched in 2000, is designed to help protect *Visa* account and transaction information, safeguarding both the integrity of operations and the goodwill of cardholders.

Merchants and service providers who implement the controls outlined in this program can benefit in numerous ways. If applied properly and consistently, these controls can help merchants:

- **GAIN** a competitive edge
- **INCREASE** revenue and improve their bottom line
- **MAINTAIN** a positive image
- **PROMOTE** consumer confidence

## BENEFITS TO MERCHANTS

Visa helps build consumer trust and increase revenue by providing merchants with tools to help prevent fraud. These tools can help merchants:

- Protect the integrity of the merchant's brand and build consumer trust by demonstrating high levels of compliance with industry standards;
- Reduce the number of cardholder disputes, thereby increasing the number of sales that positively impact the bottom line;
- Improve data security awareness and knowledge and help merchants strengthen security measures to minimize the possibility of data security attacks;
- Minimize data exposure and loss in the event of a security breach; and
- Access information about industry best practices and *Visa* services such as security bulletins.

## SECURING DATA MAKES GOOD BUSINESS SENSE

Tighter security benefits everyone. Protecting data is a good business investment. It may be difficult to quantify the return on investment for security-related costs as they have no direct effect on the bottom line. However, the potential cost of *not* securing data is far greater. Any merchant that has suffered a data security breach knows from hard experience the consequences of such an attack:

- Financial losses
- Reputation damage
- Exposure to legal risks
- Loss of business opportunities as a result of lack of trust
- Down time resulting from a data security breach
- Potential payment scheme fines, penalties, fees or termination of facility
- Cost of a forensic review

Visa listened to the needs of the merchant community in developing a practical yet comprehensive program that helps protect sensitive *Visa* account information — the AIS Program.

## WHAT IS AIS?

The Account Information Security Program is a compliance validation program that requires anyone who stores, transmits or processes *Visa* account data — financial institutions, merchants, Acquirers and Processors — to assess whether cardholder data is secure within their organization. The program's standards-based, proven methodology then enables organizations to improve their level of security to meet or exceed industry standards.

Whether data resides on a stand-alone server or on a merchant website, the AIS Program works to protect data at all points in the payments system.



For merchants, the AIS Program helps evaluate and improve organizational, physical and logical controls over data security. It is a requirement for all merchants participating in the *Visa* acceptance environment. AIS standards address things such as cryptographic operations, logical access controls, physical data protection and network security.

Under the AIS Program, all merchants who store, transmit or processes *Visa* account information are required to do so in a safe and secure manner, as per the Payment Card Industry (PCI) Data Security Standard. Participation in this program will give merchants timely access to information and best practices relevant to data security.

## HOW DO AIS AND PCI WORK TOGETHER?

To be compliant with the AIS Program, merchants and service providers must adhere to the PCI Data Security Standard (DSS). This standard is a result of industry collaboration and is designed to create common industry security requirements. The AIS Program requires merchants and other service providers that come into contact with sensitive cardholder data are PCI DSS compliant. Select merchants must validate compliance in accordance with the AIS Program's implementation framework.

The PCI Data Security Standard consists of 12 basic requirements. For more detailed information about these requirements or to download a PDF version of the standard, please visit [www.visa.ca/ais](http://www.visa.ca/ais).

### Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

### Protect Cardholder Data

3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.



### **Maintain a Vulnerability Management Program**

5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

### **Implement Strong Access Control Measures**

7. Restrict access to sensitive cardholder data on a business need-to-know basis.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

### **Regularly Monitor and Test Networks**

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

### **Maintain an Information Security Policy**

12. Maintain a policy that addresses information security.

## DOES THE AIS PROGRAM APPLY TO ME?

All merchants who are involved in the *Visa* payment process are required to be compliant with the PCI Data Security Standard. The standard is the foundation for the Account Information Security Program.

Requirements for validation of AIS Program compliance are based on the volume of transactions processed by a merchant and, therefore, the potential risk and exposure introduced into the *Visa* system.

Acquirers are responsible for determining the compliance validation requirement levels of their merchants. All merchants will fall into one of the four merchant levels based on the annual *Visa* transaction volume of that merchant. For more information about merchant levels, please visit [www.visa.ca/ais](http://www.visa.ca/ais).

We are here, along with your Acquirer, to help guide you through the most efficient and cost-effective way to comply with the AIS Program. A Visa-approved Qualified Security Assessor (QSA) can help guide you through the process, cut down on the guess work and reduce the time required for compliance. These approved QSAs can administer the validation process directly with the merchants on behalf of the Acquirer, and assure confidentiality. Contact your Acquirer or visit [www.visa.ca/ais](http://www.visa.ca/ais) for more information on approved QSAs.



## HOW DO I ENROL?

The AIS compliance program may include some or all of the following elements, depending on the merchant's volume of transactions:

1. Online enrolment
2. Online completion of a self-assessment questionnaire
3. Remote vulnerability testing of the merchant's systems by a QSA
4. On-site review
5. Online Final Report of compliance by a QSA
6. Remediation Action Plan

If a brick-and-mortar, e-commerce or mail order / telephone order (MOTO) merchant is required to validate compliance, they are required to enrol with a Qualified Security Assessor, undertake an annual self-assessment questionnaire and complete a quarterly network scan, which must be validated by a QSA. In order to fulfill Visa's AIS requirements, some merchants will also have to undertake an on-site PCI Data Security Assessment to ensure adherence to the industry-wide PCI standard that is a part of Visa's AIS compliance.

For more detailed information about compliance requirements and validation procedures, please visit [www.visa.ca/ais](http://www.visa.ca/ais).

Customer trust takes a long time to build. Don't lose it overnight.

## "SAFE HARBOUR": COMPLIANCE PROTECTION

Merchants deemed to be AIS compliant will be granted "safe harbour" from any penalties, fees and fines by Visa Canada in the event of a hack or compromise. This applies to any merchants who have validated their AIS compliance according to the implementation framework and are deemed by a Visa-approved Qualified Incident Response Assessor's post-compromise forensic investigation to have been AIS compliant at the time of the data security breach.

## LAYERS OF PROTECTION WORKING TOGETHER: SECURITY IS EVERYONE'S RESPONSIBILITY

Visa and its *Visa*-issuing financial institutions recognize that, as business dependencies on technology continue to grow at an increasing pace, exposure to the wave of potential security threats mounts day by day. Visa is committed to working with the merchant community to ensure the security of the entire *Visa* payment system.

Through significant investments in technology and the cooperative efforts between Visa and partners such as the merchant community, the incidence of *Visa* system fraud has stayed low even as the volume of *Visa* card transactions has grown dramatically. Visa's technology and experience work to keep all participants in the *Visa* payment system one step ahead of criminals and ensures "seamless security" — in other words, every transaction is protected from end to end, so that no matter where you are in the transaction process, there are security measures in place to protect *Visa* cards and accounts.

## ABOUT VISA

Visa operates the world's largest retail electronic payments network and is one of the most recognized global financial services brands. Visa facilitates global commerce through the transfer of value and information among financial institutions, merchants, consumers, businesses and government entities. We offer a range of branded payment product platforms, which our financial institution clients use to develop and offer credit, charge, deferred debit, prepaid and cash access programs to cardholders. *Visa*'s card platforms provide consumers, businesses, merchants and government entities with a secure, convenient and reliable way to pay and be paid in 170 countries and territories.



® /™ Registered Trademarks / Trademarks of Visa International;  
Visa Canada is a licensed user.