SOLUTION GUIDE

BECOMING PCI-DSS COMPLIANT

WHAT IS PCI-DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The standard, uses as its foundation the 12 PCI DSS requirements, and combines them with corresponding testing procedures into a security assessment tool.

WHO IS IT FOR

All companies that accept credit cards as payment must be compliant with PCI-DSS regulations. Merchant requirements vary depending on the Level/Tier (or size) of the company and the merchant type.

Level	Criteria
1	**Greater than 6M Visa transactions / Year** or Global L1 merchants
2	**1 million to 6 million Visa transactions / Year**
3	**20,000 to 1M Visa e-commerce transactions / Year** [~100/Day+]
4	**Less than 20,000 Visa e-commerce transactions / year** or All other merchants - up to 1M Visa transactions / Yr

* Compliance is required by Merchant (and their 3rd party service providers)

Merchant type defines the methods used to accept, process, store and manage the personal private data card data.

Merchant Types				
Type 1	**Type 2**	**Type 3**	**Type 4**	**Type 5**
All Cardholder Data Outsourced	Imprint Only No Electronic Storage	Dial-out Terminals No Electronic Storage	POS Internet System No Electronic Storage	All Other Merchants (Local Data Storage)
LOWER	Certification Requirements →			**HIGHER**
LOWER RISK	Risk →			**HIGHER RISK**

WHY IS DATA PROTECTION IMPORTANT

In 2017 there were at least 150,000,000 personal private data records breached. The main industries affected by data breach are: medical, education, government, financial and retail. All of these industries and most businesses now sell products directly and therefore take credit cards.

All Data Breaches (2009-9/2010)

Events	# of Reported Records
410	150,000,000+

Source: Privacy Rights Clearinghouse

The biggest threats to personal private data include: portable devices and storage, insider (mostly employees) intentional and unintentional breaches, misuse of physical documents, hackers and stolen data off servers.

VISA and MasterCard both can impose fines (up to $200,000 per occurrence) for breaches or non-compliance. Other potential risks include: lawsuits, lost productivity and requirements to publically disclose breaches.

PCI SOLUTIONS FOR MERCHANTS

PCI solutions for merchants must include several components including selection of the correct Self Assessment Questionnaire, quarterly scans, and attestation of compliance. To become validated merchants must possess the right security product, process and policies to meet the PCI-DSS standard.

eSecurity Solutions can help you navigate this process and make sure that you have done all that is possible to reduce the risk of violations or data breach.

Services Needed by Merchants	eSecurity Solutions
PCI Security Assessment	✓
SAQ & A Process Support	✓
Quarterly Network Scan (or Daily with Logo)	✓
Security Products	✓
Security Product Install & Configuration	✓
Penetration Tests (Type 5)	✓