INNOVATION THAT PROTECTS

SMART DATA SECURITY FOR PARKS & REC MANAGEMENT

ACTIVE network

658_14

Introduction

A major data security breach still makes headlines, but it no longer surprises most consumers. Internet mayhem and identity theft are now a universal part of the relentless, illegal pursuit of data.

Consumers can take steps to protect themselves, but once they engage with an organization, the obligation to protect their information lies with the new owner of their data—You.

Many people may feel that, as part of city governments, Parks and Recreation departments' data security is implied, but that's not always the case. Many government offices are not up-to-date with the latest security for its citizens' financial data.

ACTIVE Network has built its reputation on maintaining the Software as a Service (SaaS) industry's best security. Protecting our customers' and their customers' data is our most important goal. We take the hassle out of security by bearing all the data security responsibility for your data.

Let us tell you how.

Contents

Know the Risk

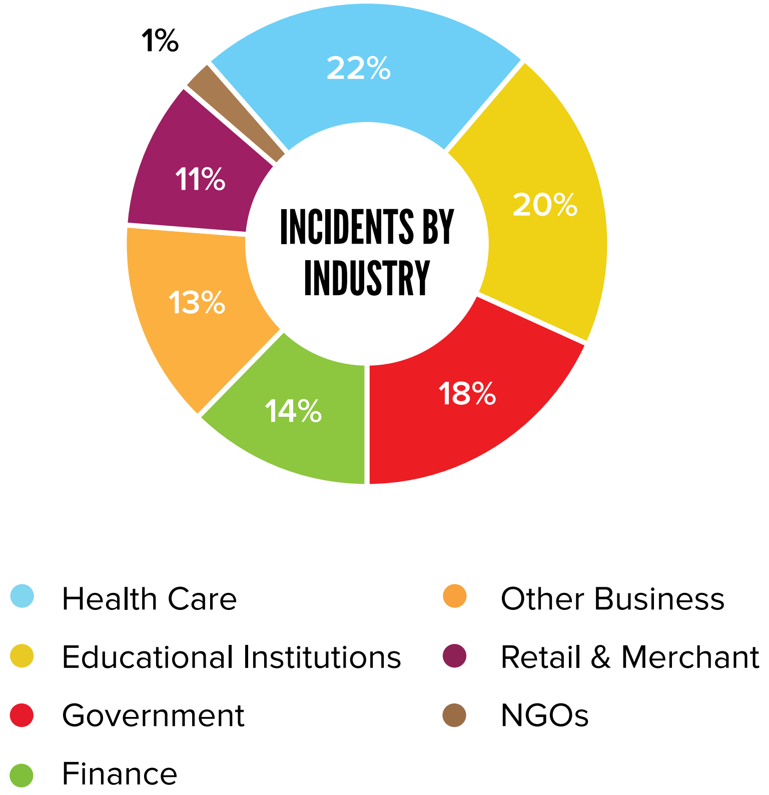
As companies collect more data, protecting it and tracking access to it is becoming a priority. Because industry data shows that 92% of data breaches are avoidable, **data protection must be a proactive concern for all businesses:**

- 93% of organizations that lose their data center for 10+ days go bankrupt within a year.
- 43% of organizations that experience a disaster never reopen.
- Only 6% of organizations without a disaster recovery plan will survive long term.

As the following chart shows, government is keeping up in the world of data breaches, accounting for nearly one-fifth of all security incidents. This is frightening when you consider that this percentage represents only incidents, not the number of individuals represented in those penetrated government databases nor the total amount of funds lost.

Governments account for nearly 1/5th of all data security incidents

-Cloudtweaks



How We Protect Your Consumer’s Credit Card

No matter the size, any organization taking credit card payments is responsible for Payment Card Industry (PCI) compliance. This involves meeting a set of specific security standards that were developed to protect card information during and after a financial transaction. All card brands require PCI Compliance, and failure to comply can result in:

- Financial Penalties and Fines
- Revocation of ability to accept payment cards
- Loss of consumer confidence
- Insurance claims
- Lawsuits, including legal costs
- Higher subsequent costs of compliance

And, of course, without PCI safeguards, your customer’s data is at risk.

Do You Have Time for This?

Minimum PCI Compliance has 6 major objectives, requiring 12 major steps. It is time-consuming, difficult, and expensive to meet these standards:

60% of security breaches can be avoided with secure data encryption and data backup.
-Cloudtweaks

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 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 for security for all personnel

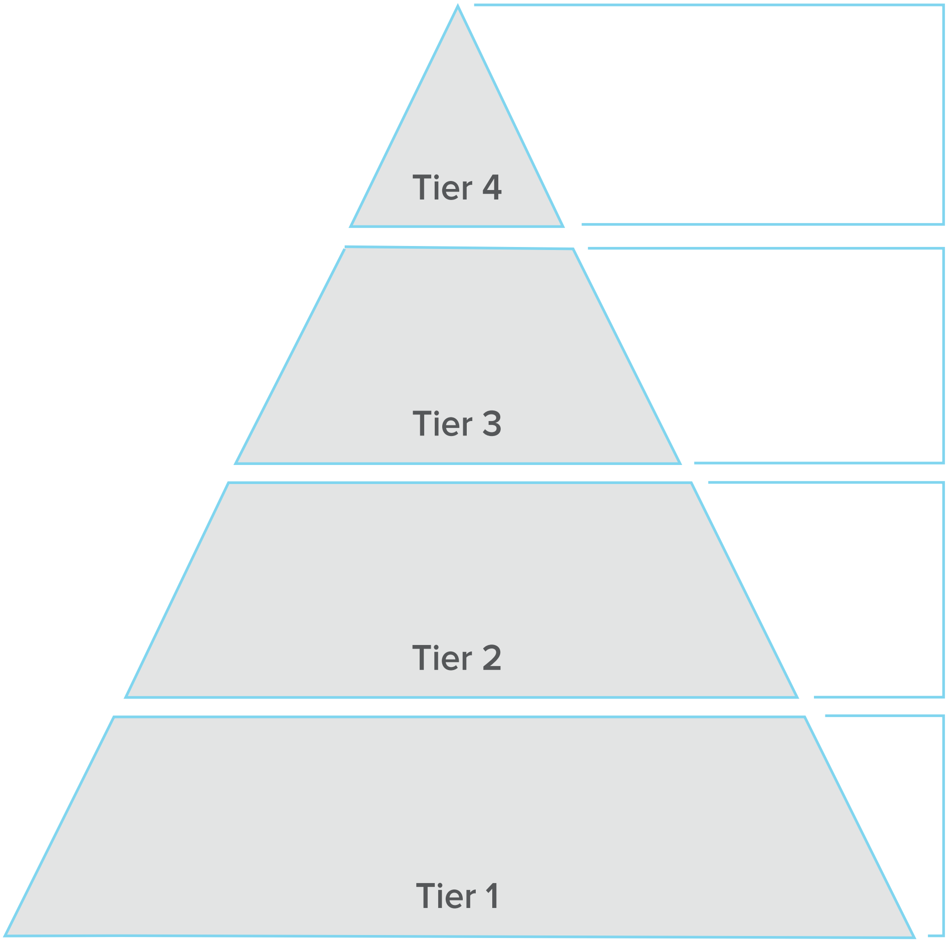
Security and the Cloud

The Cloud is growing and is the most popular—and arguably safest—way to store data.

Small, cash-strapped government organizations simply cannot afford the kind of security needed today. Even if their data is stored in a certified data center, they are often ineligible for the redundancy of data, power, and cooling that is available to larger and Enterprise-level corporations, as this diagram illustrates:

ACTIVE has been not only operating but also mastering Cloud-based technology for over a decade. New players to the Cloud simply cannot claim the superior level of security that comes with ACTIVE's experience, growth, and long-term success.

DATA CENTER TIERS

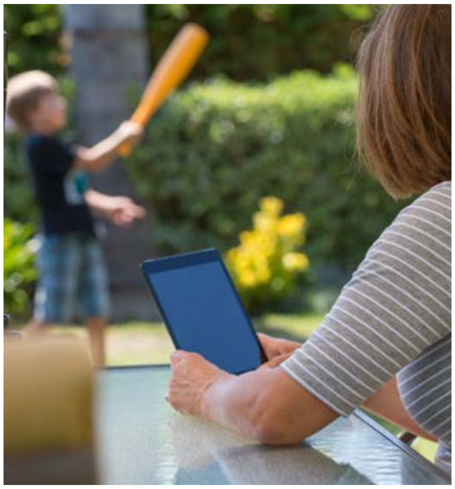


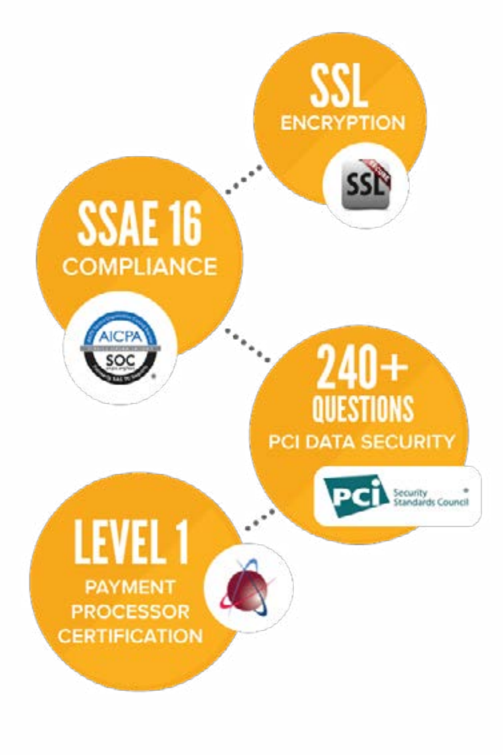
- Enterprise Corporations
- 99.995% Uptime
- 2.4 Minutes Downtime Per Year
- 2N+1 Fully Redundant
- 96 Hour Power Outage Protection

- Large Businesses
- 99.982% Uptime
- 1.6 Hours Downtime Per Year
- N+1 Fault Tolerant
- 72 Hour Power Outage Protection

- Medium-Size Businesses
- 99.749% Uptime
- 22 Hours Downtime Per Year
- N+1 Fault Tolerant
- Partial Redundancy in Power Outage

- Small Businesses
- 99.671% Uptime
- 28.8 Hours Downtime Per Year
- No Redundancy





ACTIVE's Data Security is Unequaled

As a Tier 4, Enterprise-level corporation, ACTIVE takes all the worry out of data collection and storage.

Credit Card Protection

Processing over $3 billion in annual credit card transactions demands we meet the highest level of PCI compliance for data security. In addition to the mandatory audit, we hold a current Level 1 Payment Processor Certification for all payment processing. Level 1 certification involves undergoing rigorous third-party assessments and testing for over 200 controls. Our PCI compliance level covers everything from network security to application security, to background screening of our employees.

When we store your financial data, **we take on the burden of PCI requirements for you,** eliminating the pain of compliance in cost, time, and other resources. No other participation management software provider can match this level of activity, experience, and, therefore, security.

ACTIVE's PCI Compliance Allows Us to:

- Protect Cardholder Data
- Maintain a Secure Network
- Operate a Vulnerability Management Program
- Monitor and Test Networks Regularly
- Maintain an Information Security Policy
- Implement Strong Access Control

State-of-the-Art Data Centers

ACTIVE operates four major data centers across North America. Operating 24/7/365 at a multi-country, multi-site level enables us to guarantee double redundancy of your data. It's how we can confidently say your data is safe.

Smart Data Security Starts with ACTIVE

Data breaches can be catastrophic but, fortunately, they can also be avoided with the right compliance and data security.

With ACTIVE, **we take the risk out of your hands.** Click on the link below to connect with us and learn how our smart approach to data security can serve your particular needs.

Let's Talk! Speak with a Parks and Rec Specialist to learn more about how you can protect your data.

888.820.5808 | ACTIVE-Communities@activenetwork.com | www.activenetwork.com