

Security and Privacy Assurance

Security and privacy are essential — ensure that your information remains confidential with Sprint Email ProtectionSM Services

Businesses of all sizes can place their trust in Sprint to protect their message systems from spam and viruses as well as to safeguard data in transit to and from their corporate networks.

We understand that your e-mail often contains highly sensitive material and that you can't afford to risk having that information compromised in any way. With Sprint Email ProtectionSM Services, we not only screen your messages upfront before they reach your e-mail server, we employ rigorous measures to provide privacy and security for your e-mail for the fraction of a second that it is in our hands.

To protect the confidentiality and integrity of customer information, the following security measures are in place at the network data centers where your e-mail is examined for spam, viruses and other threats.

Physical security

The physical premises are guarded and under video surveillance 24 x 7. Each data center is certified with the American Institute of Certified Public Accountants' SAS 70 standards. This certification ensures that the data centers have passed stringent third-party tests and demonstrate processes and mechanisms necessary to securely host and exchange sensitive data for their customers.

Data security

All data traversing the Sprint network is encrypted. Access to that data is also restricted based on strictly enforced policies. These policies ensure that detailed logs are maintained for data traversing the network, including logins and access to data.

Legitimate e-mail is never stored permanently. With Sprint Disaster Recovery Service, e-mail is queued until your network is available to receive e-mail.

Application security

All application and server interfaces are password protected over SSL-encrypted tunnels. The SMTP servers use Postfix, a secure, stable and highly scalable SMTP server. DNS security is maintained by the latest version of BIND with new releases tested and installed as they become available. External DNS resolvers are run on dedicated hardware in a chrooted environment to mitigate any BIND security concerns.

Personnel security

Data center staff adhere to strict policies and procedures. Employees must successfully complete background checks, and all staff logins are recorded for audit purposes.



One Sprint. Many Solutions.SM

Voice/Data

PCS Wireless

Internet Services

E-Business Solutions

Managed Services

The Sprint benefit

Bottom line, with Sprint Email Protection Services, you can be protected from viruses and other e-mail-borne threats that could wreak havoc with your corporate data and have confidence that your e-mail is in exceptionally safe hands.

Why Sprint?

When you choose Sprint, you're in good company. More than 90 percent of the Fortune 500 chooses Sprint for data, Internet, voice and wireless solutions.

When you select Sprint, you're doing business with a global company that:

- Has a rich heritage more than a century strong and remains one of the most financially stable companies in the telecom industry
- Can meet virtually any communications need through a broad portfolio and interoperable network infrastructure, allowing for fully integrated custom solutions for your business
- Is committed to developing solutions that can transform the way you get business done
- Has won industry and customer accolades for service reliability, cost effectiveness, customer satisfaction and product innovation

**Please contact your
Sprint Sales Representative
or Authorized Sales Agent.**

**1-877-700-8919
www.sprintbiz.com**

