

Integris.

**Don't be
a sitting
duck** 

15 urgent security protections every
business should have in place now

Integris.

15 steps to get you on the right road for cyber insurance



Endpoint Detection & Response

Protect your computers from malware, viruses, and cyberattacks with artificial intelligence (AI) based endpoint security. Today's latest technology (which replaces your outdated antivirus solution) protects against file-less and script-based threats and can even roll back a ransomware attack. All this monitored by a 24x7 Security Operations Center (SOC).

In place Need to put in place



DNS Filtering

Internet security is a race against time. Cloud-based security detects web threats as they emerge on the internet, and blocks them on your network within seconds – before they reach the user.

In place Need to put in place



Security Incident & Event Management

Uses big data engines to review your device's security logs, which protects your network from threats and improves compliance.

In place Need to put in place



Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

In place Need to put in place



Threat Hunting

Find and stop hidden threats that sneak past preventive security. Real time workstation monitoring for evidence of compromise.

In place Need to put in place



Business Continuity & Disaster Recovery

Prevent data loss and minimize downtime by using a reliable solution that you can count on in a disaster. It will allow you to recover in a disaster and keep your recovery time to a minimum. Your M365 email, SharePoint, OneDrive data also needs to be protected.

In place Need to put in place



Email Encryption

Service that encrypts emails and attachments at rest, and in transit, working equally well for desktop and mobile devices.

In place Need to put in place



Firewall

Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet.

In place Need to put in place



Dark Web Monitoring

Monitor threats and vulnerabilities 24/7/365 and receive alerts before a breach occurs. Identifying any compromised or stolen data and closing security gaps fast.

In place Need to put in place



Email Phishing Protection

Email security platform that is continuously learning, detecting, and remediating every threat that reaches your email inbox, both before and after delivery. Suspicious emails and links within are quarantined. If an employee clicks a bad link, no worries.

In place Need to put in place



Password Manager

A password manager to remove obstacles, letting you get back to work. Apply security policies, save unique passwords for every login, generate strong passwords, and share effortlessly and securely.

In place Need to put in place



Multi-Factor Authentication

Utilize MFA whenever you can on your network infrastructure. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

In place Need to put in place



Email Spam Filtering

Secure your email from cyberattacks. Iconic can help you choose a service that will filter out the dangerous spam that clogs your employee's inboxes.

In place Need to put in place



Security Patching

Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers and servers from the latest known attacks.

In place Need to put in place

Don't know? Need to fill in the gaps? Reach out to get secure.

Getting cyber insurance is becoming more complicated. Carriers are requiring more for coverage every day.

These 15 steps will get you started on the right road to coverage. They're also necessary to protect your company from attacks in the first place.

Don't know where to start? Integris can help. Our assessment can identify what your organization needs, and our team can help fill in the gaps.

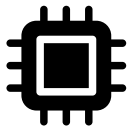
Reach out today to get secure:

integrisit.com/contact

What Biden's Executive Order on cybersecurity means for your organization

Joe Biden's executive order on cybersecurity is a landmark directive aimed at tightening cybersecurity procedures for government agencies and contractors. We believe it's a preview of the kinds of standards all companies will need to adhere to in the very near future. Don't be one of those companies struggling to keep up. Get ahead of the curve by using our checklist to assess the strengths and weaknesses of your cybersecurity protocols.

Identify your risk with our Security Assessment



Based on NIST Framework

We base our assessments on the internationally recognized NIST Cybersecurity Framework.



Easy-to-Understand Results

You can truly understand your results, because we craft our assessments with common language for clarity.



Actionable Remediation

We include remediation recommendations to help create an actionable plan for your business.

Request your security assessment today!

integrisit.com/contact

"It is great to have an IT company that will take a problem off your hands and take care of it from beginning to end."

Mike T., Financial Business