



Sirtawn Systems

Start Fighting Cyber Crime with Knowledge and Action.

Our Newsletter for Issue #175 is dedicated to AI Network Concerns.

**Artificial Intelligence!
It will affect your Business.**

Why is your network the BACKBONE of your business?

1. Keeps your operations running smoothly by connecting employees across departments and locations, fostering collaboration.
2. Makes file sharing easy, streamlining operations for efficient teamwork.
3. Secures and stores important information for easy access, ensuring smooth operations and peace of mind.
4. Allows instant data access and real-time collaboration among your teams, boosting productivity.
5. Provides quick access to databases and essential applications, making tasks more efficient.

Key Elements of a complete Data Security Policy.

- Safeguard Data Privacy.

- Password Management.

- Internet Usage.

- Email Usage.

- Company Devices.

***Safeguard:** Apart from complying with the existing rules & regulations, a privacy policy will guide your employees on how to handle sensitive information in such a way that is not compromised.

***Passwords:** Setting up a password policy will ensure your company Resources are protected and only accessible by authorized personnel. The guidelines should include password length, complexity and how often it needs to be changed

***Internet:** An internet usage policy that defines best practices while accessing the internet, such as restricting employees from visiting certain sites or prohibiting unnecessary file downloads, will help set limitations and minimize security risks.

***Email Usage:** Companies often fall victim to data breaches due to employee negligence or email misuse. With an email policy in place, your employees will be aware of what is expected of them and how company information should be disseminated internally.

***Company Devices:** As the use mobile devices for work gains momentum, it also opens the door to several security threats. Implementing a comprehensive policy will help mitigate the risks associated with data theft and stolen devices.

Key Elements of a complete Data Security Policy

Personal
Employee Devices.

Social Media
Presence.

Software User
Agreements.

Reporting Security
Breaches.

Employee Devices. Unlike company-owned devices its difficult to have complete control over personal devices. A security policy, such as accessing company resources only through a secure VPN or installing an antivirus or mobile device management software will set certain boundaries or limitations.

Social Media. Protecting your company's reputation is critical not only within the workplace but outside as well. A social media policy will help you regulate your employees' online actives.

Software Agreements. Violating a software license agreement can lead to legal implications. A software user agreement policy will ensure your employees comply with the procedures regarding the appropriate use of company-owned software.

Reporting Security Breaches. Implementing a Security Incident Reporting policy is important to minimize negative impacts. Your employees should be educated on how to report real or suspected security breaches and what steps they need to take to prevent the from happening.

Data Security Risks can arise at any time and from anywhere!

Your Network + Data Security is the Backbone of your business. All elements must be protected to completely protect your business and your future.

AI is the next frontier... good or bad.

Ethical vs Unethical:

AI is a double-edged sword in the digital realm. Learn to wield it with integrity and safeguard your business.

Now that we've identified the importance of your network and the key elements to provide complete Data Security Policy the following displays the difference between Ethical and Unethical use of AI.

Ethical:

PERSONALIZATION:

Enhances customer experiences with tailored support.

OPTIMIZATION:

Streamlines operations, predicts failures and automates tasks.

IDENTIFICATION:

Uncovers hidden trends for informed business decisions.

PROTECTION:

Vigilantly detects fraud and secures assets.

Unethical:

AGRESSION:

Powers cyberattacks, increasing their complexity.

INTRUSION:

Collects data, potentially breaching privacy.

MANIPULATION:

Crafts targeted disinformation campaigns.

DECEPTION:

Generates deepfakes, fostering misinformation.

4 Ways AI can Strengthen your business security.

Hackers are using AI to target businesses like yours. It's time to use the enemy's tactic against them. Leverage AI proactively to stay ahead of malicious actors.

01 Continuous Monitoring: AI keeps an eye out for anything out of the ordinary.

02 Quick Risk Mitigation: AI can quickly detect and contain a risk.

03 Automate Responses: AI can reduce damage by automatically blocking anything suspicious.

04 Gets Smarter Over Time: AI continuously learns from past threats and adapts itself to identify emerging threats.

Ready to discover how AI can empower your business?

Contact us!

The Future of AI will change the World...a few ways: Some good and some bad...

Improved Business Automation: AI's ability to analyze massive amounts of data and create a visual format for decision-making process is a huge step forward.

Data Privacy Issues: As volumes of data increase, so does the required security. AI provides multiple methods to secure that security regardless of the volume.

Climate Change: AI can analyze massive climate issues (data) and help select the best alternatives to stabilize the climate and other associated problems such as transportation and climate technology.

AI in Manufacturing: AI has been present in manufacturing for many years specifically in robotics, production tracking and required inventory.

AI in Medicine & Healthcare: AI has been used in disease identification, Drug testing and many other areas that require serious analytics.

Other areas using AI include: Finance (Banks, Loans), Media (Auto writing), Customer Service (Virtual Assistants), Transportation (Best Routes, Streamline Service).

Miss Use of AI will affect Jobs, Deepfakes, Data Privacy and many other criminal activities.

Our Assessment Offer



This monthly publication provided courtesy of Barry Brown, President of Sirtawn Systems.

FIGHTING CYBERCRIMINALS ON YOUR OWN CAN BE TIRING WHEN YOU HAVE A BUSINESS TO RUN.

CONTACT US TODAY

FIND OUT WHAT IT'S LIKE TO HAVE OUR CYBERSECURITY EXPERTS IN YOUR CORNER.

We are offering a FREE Network Security Audit with no obligation. You will receive a "Cyber Security Audit" outlining our findings following the audit. Again ... **NO Obligation....**

Sirtawn Systems

Your Cyber Security Experts

Phone: (905) 947-1636

Website: www.sirtawn.com

Email: sirtawnsystems@gmail.com