MATT BACAK'S CHECKLIST

Checklist 17 - Implementing DNS Security And Antivirus

Project Name: _____ **Date:** _____

	Yes	No

The domain name system refers to a protocol that enables the use of domain name thus enabling internet usability. The DNS is commonly targeted by attackers due to its ability to pass through firewall networks without objections. One limitation of DNS is that it was not developed with security in mind and this therefore exposes it to exploits such as Denial of Service attacks (DoS), DNS hijacking, DNS DDoS Amplification, and on-path attacks. The lack of integrated security in DNS' design has prompted the development of varied measures aimed at enhancing its security. The DNS Security Extensions (DNSSEC) is one of the measures developed to mitigate attacks by ensuring validity by signing data digitally.

In a similar vein, it is essential to install antivirus software to protect the computer against viruses, malware, worms and Trojan horses. The antivirus software monitors applications, software, web pages, files and networks for potential threats and flags any suspicious or inappropriate behaviors. This checklist provides tips for the implementing of DNS security and antivirus.

Part 1 – DNS Security

1	Implement firewalls to prevent unauthorized DNS access.	☐	☐
2	Use DNS forwarders.		

Notes

MATT BACAK'S CHECKLIST

Checklist 17 - Implementing DNS Security And Antivirus

3	Ensure zone transfers are disabled.	☐	☐
4	Enable DDNS for secure connections only.	☐	☐
5	Configure access controls on DNS registry entries.	☐	☐
6	Use hidden DNS servers and.	☐	☐
7	Optimize DNSSEC to validate DNS data integrity.	☐	☐
8	Resolve names for domains by using DNS resolvers.	☐	☐
9	Check that DNS logging is enabled.	☐	☐

Notes

MATT BACAK'S CHECKLIST

Checklist 17 - Implementing DNS Security And Antivirus

10 Lock DNS cache to protect the DNS from cache pollution. ☐ ☐

11 Block malicious domains by filtering DNS requests. ☐ ☐

Part 2 – Implementing Antivirus Software

12 Identify the needs of your organization. ☐ ☐

13 Ensure the antivirus comes with download protection. ☐ ☐

14 Ensure compatibility with your system. ☐ ☐

15 Evaluate the software's privacy policy. ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 17 - Implementing DNS Security And Antivirus

16 Check the antivirus' ability to detect and remove malware and viruses. ☐ ☐

17 Analyze the software's quick scan feature. ☐ ☐

18 Check the software's backup capabilities. ☐ ☐

19 Determine whether the solution anticipates both your current and future needs. ☐ ☐

20 Check that the antivirus is user-friendly. ☐ ☐

21 Check that there are additional protective features. ☐ ☐

22 Review the software's tech support. ☐ ☐

Notes

Checklist 17 - Implementing DNS Security And Antivirus

Notes:

Antivirus options in the market include the following:

•Kaspersky Security Cloud Free
•Microsoft Windows Defender
•Avira Free Security
•AVG AntiVirus Free
•Bitdefender Antivirus Free Edition
•Avast Free Antivirus

Notes