Amidata

The ABP 11

AMIDATA BEST PRACTICE: 11 CRITICAL CYBERSECURITY CONTROLS FOR BUSINESS SURVIVAL

amidata.tech

At a time when businesses are facing significant cyber threats, Amidata has your back.

We adhere to an 11-point best practice framework to provide end-to-end cybersecurity protection for your internet-connected technology network. So, you can focus on your business while we take the critical preventative measures required to secure your data, systems, and reputation.

WHAT ARE THE 11 MOST CRITICAL CYBERSECURITY MEASURES YOU CAN TAKE?

1 

ENDPOINT SECURITY – Secure your user devices and cloud endpoints with next-generation endpoint security, ensuring ongoing cyber protection for your users and IT assets.

2 

EMAIL SECURITY – Apply best practices to protect your business users and their accounts from email-based security threats such as scams and phishing attacks.

3 

ENFORCE APPLICATION CONTROL – Block non-approved software or code, ensuring only approved applications can be installed or accessed, preventing the execution of dangerous malware and ransomware.

4 

RESTRICT ADMINISTRATIVE PRIVILEGES – Limit administrative privileges to only those who require them for specific tasks, reducing the chances of cyber criminals gaining unauthorised access to your IT network.

5 

PATCH OPERATING SYSTEMS – Ensure prompt patching of operating systems as a priority to limit any potential downtime in the event an unpatched vulnerability is exploited.

6

PATCH APPLICATIONS – Pro-actively reduce your risk exposure to the 25,000 new software security vulnerabilities discovered every year by enabling the ability to identify and apply priority patches to applications.

7

HARDEN USER APPLICATIONS – Block browser access to untrusted applications and code to prevent the introduction of malware and security threats from social engineering and phishing techniques.

8

MANAGE MACROS – Restrict and manage the use of Microsoft Office macros to prevent the downloading and execution of dangerous malware and ransomware.

9

MULTI-FACTOR AUTHENTICATION – Adopt multiple, distinct types of personal identification to ensure that users are who they say they are, preventing unauthorised access to your systems.

10

DAILY BACKUPS – Implement 100% reliable offsite and encrypted daily backups to mitigate the financial and business impact of a data breach or cyber-attack.

11

CYBER AWARENESS TRAINING – Provide continuous and up-to-date cybersecurity and best practice training for your staff to ensure vigilance and responsiveness to security threats.

Best cybersecurity practice, better outcomes

To find out how to improve your cyber resilience, please ask us about ABP 11 and our proven best practice services and solutions.

Amidata

Protect your data, protect your reputation.
Contact Amidata today on **1300 426 432**,
email us at **sales@amidata.tech** or visit **amidata.tech** today.

Amidata is an Australian-based international company offering specialist data protection services. We help you ensure that your valuable data resources are always secure, backed up and performing at their best. We offer advice, solutions and support, along with a utility-based pricing model. This will help you break free of resource constraints and give you the peace of mind of knowing that your data is fully protected.

Amidata Head Office
6/123 Chesterville Rd
Highett, Victoria, 3190

Amidata Sydney
17/122 Arthur Street
North Sydney, NSW, 2060

Amidata UK
24 Wellington Court,
Brighton Marina,
East Sussex,
England, BN2 5WE

Amidata Philippines
Unit 707, 7th Floor,
One Park Drive, 11th Drive
Corner 9th Avenue, BGC,
Taguig, Philippines