NATIONAL VETERINARY LAW GROUP AT
MANDELBAUM BARRETT PC

What Should Be Included in a Veterinary Clinic's Information Security Policy?

Introduction: As dedicated members of our clinic, safeguarding our digital integrity is as crucial as our patient care. The below policies should be followed to help create a secure cyber environment.

Section 1: Strong Passwords

Create unique passwords combining upper- and lower-case letters, numbers, and special characters. Fortified passwords deter unauthorized access. The use of multi-factor authentication should be a requirement, not an option.

Section 2: Vigilance Against Phishing

Exercise caution with suspicious emails and links. Verify sources to prevent divulging personal information.

Section 3: Device Security

Lock screens and secure devices to prevent unauthorized access and data breaches.

Section 4: Responsible Data Handling

Dispose of sensitive files securely. Keep the digital environment clutter-free and secure.

Section 5: Regular Software Updates

Routine updates patch vulnerabilities, enhancing overall security.

Section 6: Firewall Protection

Maintain an active firewall to ward off unauthorized access.

Section 7: Laptop Security

Protect laptops from theft or exposure in public settings.

Section 8: VPN Usage

Use a VPN for secure remote work.

Section 9: Controlled Admin Access

Limit admin access to authorized personnel only.

Section 10: When an Employee Leaves the Clinic

Ensure that centralized logging and archiving of all devices for 24 months.

Section 11: 3rd Party Providers

When using a 3rd party service provider, accredited and certified IT providers are required.

Section 12: Incident Response

Report breaches promptly to ensure efficient mitigation.

Conclusion:

Thank you for upholding our clinic's cybersecurity. Your commitment maintains a safe digital space for our patients and operations.