NBN Atlas Security Statement

The NBN Atlas takes the security of its systems and data seriously, especially for access-controlled or sensitive species data. Below is a summary of the key security measures currently in place and planned improvements:

1. Password Storage and Encryption

- Passwords are never stored in plain text.
- Since the most recent authentication upgrade, all passwords are stored using BCrypt, a secure one-way hashing algorithm designed specifically for password protection.
- Older passwords, previously encrypted with MD5, were migrated to BCrypt upon user login or password change, ensuring all current passwords meet the newer standard.

2. Brute Force Protection and Session Security

- Temporary account lockouts are triggered after repeated failed login attempts to protect against password-guessing attacks.
- Automatic session timeouts ensure that inactive user sessions expire after a period of inactivity, reducing the risk of unauthorized access if a user leaves a session open.

3. Data Protection and HTTPS Enforcement

- All traffic to the Atlas, including access to restricted data, is encrypted via HTTPS.
- Sensitive and access-controlled data cannot be indexed by search engines because access requires authentication and authorization.

4. Password Strength and Authentication Enhancements

- Strong passwords are supported but not currently enforced. We are reviewing options for stronger password requirements, particularly for accounts with access to restricted data.
- The upcoming upgrade to our authentication system will include support for modern authentication standards (e.g., OIDC, JWT) and will enable the option for Multi-Factor Authentication (MFA).

5. Next Steps

- The authentication system is being upgraded again before end of 2025
- We expect to introduce MFA enforcement options as part of this upgrade.
- Guidance and advice for users seeking data via Access Controls to include details of password requirements and MFA when published.