The Integrated Policy Framework

Traditional security policies fail because they prescribe specific methods rather than focusing on outcomes. An accessibility-centred approach defines security objectives while allowing flexible methods of achievement:

1. Outcome-Based Policy Design

Traditional Policy: 'All users must use the corporate password manager to generate and store complex passwords with minimum 16 characters including uppercase, lowercase, numbers, and symbols.'

Accessibility-Centred Policy: 'All users must maintain unique, strong authentication credentials for each system. The organisation provides multiple secure methods for credential management, including [list of accessible options].'

2. Equivalent Security Pathways (multiple approaches that achieve the same security goal through different mechanisms)

Example: Multi-Factor Authentication

Multiple equivalent secure paths:

- Standard Path: Authenticator app generating time-based codes
- Alternative Path 1: Push notification with accessible interface
- Alternative Path 2: Hardware token with tactile interface
- Alternative Path 3: Biometric option with non-biometric fallback

Organisations implementing accessibility-centred security policies report higher compliance rates compared to those with traditional policies. This isn't surprising; policies that can be used by everyone are more likely to be followed by everyone.