Cyber Security Policy

Security controls for laptops, cloud services, client data and creative production assets.

Document reference	BC-POL-010
Version	2.0
Status	Approved for publication
Approval date	08 August 2026
Next review	08 August 2027

Legal entity: Becks & Clates Ltd | Company number: 15821561
Registered office: 320 Firecrest Court, Centre Park, Warrington, WA1 1RG
Approved by: Director, Becks & Clates Ltd

Document control

Document title	Cyber Security Policy
Reference	BC-POL-010
Owner	Director
Approved by	Director, Becks & Clates Ltd
Version	2.0
Effective date	08 August 2026
Review cycle	At least annually and following material legal, operational or organisational change

Document status: public. Printed copies are uncontrolled. The version published by Becks & Clates is the current controlled version.

Contents

Security commitment

Becks & Clates uses a digital-first operating model and depends on laptops, cloud platforms, email, production storage and online client services. Cyber security is therefore a core operational and client-risk control.

The objective is to reduce the likelihood and impact of account compromise, malware, phishing, data loss, unauthorised disclosure and disruption.

Identity and access management

- Unique user accounts are used for business systems where supported.
- Multi-factor authentication is enabled for important cloud services where available.
- Passwords must be strong, unique and not knowingly reused across sensitive services.
- Password managers are preferred to storing passwords in unsecured notes or messages.
- Access is removed or changed promptly when a person no longer requires it.
- Shared accounts are avoided where individual accountability is reasonably available.

Devices and software

- Business laptops and phones used for sensitive work must use screen locks and appropriate device encryption where supported.
- Operating systems, browsers and key applications are kept on supported versions and patched in a reasonable timeframe.
- Security software and built-in protections are not intentionally disabled without a legitimate technical reason.

- Software should be sourced from legitimate vendors and unnecessary applications removed.
- Lost or stolen devices must be reported promptly so accounts and data can be protected.

Email, phishing and payment fraud

- Unexpected links, attachments, credential requests and payment-change instructions are treated cautiously.
- Changes to supplier bank details or unusual payment requests are independently verified using a trusted contact route.
- Credentials and MFA codes must not be disclosed in response to unsolicited requests.
- Suspicious messages should be reported rather than forwarded widely.

Client files, footage and cloud services

- Client material is stored in approved business systems or controlled project storage, not unnecessarily scattered across personal services.
- Public sharing links are limited in duration or access where the platform permits and sensitivity warrants it.
- Highly sensitive projects may require client-specific controls, encrypted transfer or restricted access.
- Backups or redundant cloud storage are used proportionate to the value and recoverability of active project data.
- Media is deleted or securely disposed of when no longer required and any contractual archive period has ended.

Remote working and networks

- Personnel should avoid handling sensitive work over untrusted public networks without appropriate security.
- Home routers and Wi-Fi should use current security settings and non-default administrative credentials where practicable.
- Screens and confidential conversations should be protected from unauthorised viewing in public or shared spaces.

Third-party and supplier security

- Cloud and software providers are selected with consideration to security, privacy, resilience and business need.
- Suppliers handling material client data may be required to provide security information or contractual commitments.
- Access granted to freelancers is limited to what they need and withdrawn at the end of the assignment.

Incident response

1. Report suspected compromise, data loss, malware, phishing success or unusual account activity immediately.
2. Contain the issue: disconnect affected devices where appropriate, secure accounts and preserve relevant evidence.
3. Assess affected systems, client data and personal data.
4. Reset credentials, revoke sessions/links and restore clean data/services as necessary.
5. Notify clients, insurers, regulators or individuals where contractually or legally required.
6. Record lessons and implement corrective actions.

Resilience, testing and improvement

- Critical accounts and recovery methods are reviewed periodically.
- Business continuity arrangements include loss of devices, cloud outages and cyber incidents.
- Security controls are reviewed annually and after a material incident or significant change.

This policy does not claim Cyber Essentials or another certification unless an independent certification has been obtained and remains current.