
INFORMATION SECURITY

Information Security and Data Protection Policy

Protecting client, company and personal information on every device, system and site.

Date 22 October 2026
Reference AC-ICT-POL-001 · Revision 00
To All employees, temporary personnel, contractors and subcontractors working for or on behalf of Accenti LLC

Issue of the Information Security and Data Protection Policy, AC-ICT-POL-001, Revision 00

Dear colleagues,

I am pleased to issue the Accenti Information Security and Data Protection Policy, effective 22 October 2026. It applies to every person who uses Accenti systems, devices or information.

Our clients share site plans, movement schedules, personnel data and contract information with us. Much of it is sensitive, and some of it affects people's safety. Protecting it is part of protecting our clients and our people.

The ICT Department is responsible for securing our systems, and every one of us is responsible for using them carefully: strong passwords, two-step sign-in, and reporting anything suspicious at once.

Please read this policy and report any security incident immediately. Compliance is mandatory.

Yours sincerely,


Ali Ahmed Dhadhaow
Chief Executive Officer
Accenti LLC



ADDRESS

Accenti Compound, Marina Hub
Marine Road, Airport Zone
Mogadishu 0100, Banadir, Somalia
T +252 615 540 606

WEB

www.accenti.com
info@accenti.com

DEFENSE INFRASTRUCTURE

MISSION SUPPORT

Information Security and Data Protection Policy

DOCUMENT	REVISION	EFFECTIVE	STATUS
AC-ICT-POL-001	00	22 Oct 2026	Approved / Issued
APPROVAL AUTHORITY		POLICY OWNER	
Accenti LLC Management		ICT Department	
APPROVED BY		APPROVED ON	NEXT REVIEW
Ali Ahmed Dhadhaow, Chief Executive Officer		22 Oct 2026	22 Oct 2027

Controlled document. Approval is evidenced by the signed and sealed cover letter. The current revision is held by the ICT Department; printed copies are uncontrolled.

Accenti LLC shall protect the confidentiality, integrity and availability of client, company and personal information, and shall handle personal data lawfully and fairly.

1 Application

This policy applies to all employees, contractors and third parties who use Accenti information, systems, email, cloud services, phones, laptops, radios and storage media, in the office, on site and remotely.

2 Mandatory requirements

- 2.1 Access control. Access shall be granted on a need-to-know basis, with unique accounts, strong passwords and multi-factor authentication. Access shall be removed promptly when a person leaves or changes role.
- 2.2 Classification and handling. Information shall be handled according to its sensitivity. Client-sensitive information, including site layouts, movement plans and personnel data, shall not be shared outside authorised recipients.
- 2.3 Devices. Company devices shall be encrypted, protected by screen lock and kept up to date. Personal devices may access Company email only if enrolled under Company controls.
- 2.4 Email and internet. Personnel shall be alert to phishing, verify unusual payment or bank-detail requests by phone, and not install unapproved software.

-
- 2.5 Personal data. Personal data of employees, clients and suppliers shall be collected only for a defined purpose, kept accurate, protected, retained no longer than necessary and shared only lawfully.
-
- 2.6 Backup and continuity. Business-critical data shall be backed up and restore tests carried out periodically.
-
- 2.7 Incidents. Lost or stolen devices, suspected breaches and phishing shall be reported to the ICT Department immediately.
-

3 Responsibilities and enforcement

The ICT Department shall secure systems, manage access and respond to incidents. Managers shall ensure their teams follow this policy. Every user shall protect the information and devices in their care. Breaches shall result in disciplinary action and, where required, notification to clients or authorities.

4 Implementation and review

Security awareness shall be covered at induction and refreshed annually. This policy is intended to align with ISO/IEC 27001 and applicable data protection law, and shall be reviewed at least annually or after a significant incident.

Think before you click. Report it fast.

Questions about this policy?

Security incidents, lost devices and suspicious messages go to the ICT Department immediately, or to the contacts below.

Operations — Somalia

Accenti Compound, Marina Hub
Marine Road, Airport Zone
Mogadishu 0100, Banadir, Somalia

Headquarters

United Arab Emirates

Contact

T +252 615 540 606
E info@accenti.com
W www.accenti.com

Policy owner

ICT Department
AC-ICT-POL-001 · Revision 00

■ On every site

Report it fast

Lost a phone or laptop? Clicked a suspicious link? Tell ICT straight away.
Fast reporting limits the damage.

info@accenti.com →





Zero harm to people, property and the environment.

Construction · Facility Management · Logistics
Asset Management & Fleet · Workforce Solutions