



Security Snapshot

Example output: initial risk triage for a small business

Item	Detail
Prepared for	AMUC Ltd (a fictional organisation)
Prepared by	Black Chili
Date	June 2026
Version	1.0
Classification	Example, anonymised

Important notice

This is an example Security Snapshot. It is based on a real engagement with the organisation, individuals and sector detail removed, and AMUC Ltd is a made-up name. A Snapshot is a limited diagnostic built from a short questionnaire, a call and the information supplied. It is professional advisory opinion. It is not certification, a penetration test, a legal opinion or a formal risk assessment.

1. Summary

AMUC holds personal data about customers and staff. That data sits on personal devices, in messaging apps and in personal AI accounts, with no central record of what is held and little control over suppliers. There is no single dramatic weakness. The problem is that nobody can say where the data is, who can see it or who it has been shared with.

We have grouped what we found into five priorities. Four are rated RED, which means start within 30 days. One is rated AMBER, which means plan the work and complete it within about 90 days. Much of the first priority is routine managed-service work for AMUC's IT provider.

2. The five priorities

#	Priority and why it matters	First step	Rating
1	Bring devices, accounts and communications under company control Customer data sits on personal laptops, messaging apps and unmanaged accounts, with no evidence of encryption, patching or vulnerability checks.	List every device and account, then move work onto managed, encrypted business laptops and Microsoft 365.	RED
2	Set clear rules for personal AI use Staff may be putting customer and commercial information into personal AI accounts the business cannot see. That is a confidentiality, data leakage and reputation risk.	Publish a short AI use rule and brief all staff.	RED
3	Limit who can see what, and hold less Senior staff can reach data beyond their role, enquirer data is kept indefinitely and sensitive data has no consent controls.	Restrict file store and email access to what each role needs.	RED
4	Put suppliers and data transfers under contract Suppliers and specialist partners hold data without signed agreements, and data crosses borders without a record.	Sign data processing agreements before any more data is shared.	RED
5	Write down what you process There is no record of what personal data is held or why, so nothing else can be properly targeted.	Start an Information Asset Register.	AMBER

A priority takes the rating of its most serious finding. Ratings are indicative and based on limited information.

Board-level attention recommended

We appreciate the reference to a director refusing to separate personal and professional data handling may have been a turn of phrase. With the initial summary as the only input, it is still a serious concern, and we recommend a board-level directive.

3. Next steps

A suggested sequence, in the order the work reduces exposure fastest. The last column shows which priority each step serves.

#	Step	Led by	Priority
First 30 days Stop the worst exposure			
1	Restrict file store and email access to the data each role needs	IT provider	3
2	Issue the board-level directive on separating personal and professional data	AMUC board	3
3	Publish an interim AI use rule and brief all staff for 30 minutes	AMUC, with Black Chili	2
4	Agree one approved messaging platform and stop personal channels for work	AMUC and IT provider	1
5	Inventory every device, account and application, and start the Information Asset Register	IT provider, with Black Chili	1, 5
By 90 days Build the controls			
6	Move work onto managed, encrypted business laptops and a configured Microsoft 365 tenant with multi-factor authentication, logging and retention	IT provider	1, 3
7	Run an external vulnerability assessment and set a patching routine	Black Chili	1
8	Sign data processing agreements with suppliers and start a record of international transfers	AMUC, with Black Chili	4
9	Build the record of processing activities and complete the data protection impact assessment covering sensitive data and AI use	Black Chili, with AMUC	2, 3, 5
By 6 months Prove it			
10	Achieve Cyber Essentials, then Cyber Essentials Plus, which adds hands-on technical verification by an assessor	Black Chili, and certification body	1
11	Write the policies and procedures: secure communications, AI use, retention, supplier onboarding and breach response	Black Chili, with AMUC	1 to 5
12	Complete the full ISO 27001-aligned risk assessment (underway)	Black Chili	5

What this is based on

A meeting and an internal email describing current data handling across customer, staff and test data, with follow-up emails in May 2026. We did not test any systems, and several points need substantiation before they are treated as confirmed. The full findings, the UK GDPR exposure mapping and the detailed remediation for each risk belong in a Security Action Plan.