CHAIN OF CUSTODY CHECKLIST

THINKING ABOUT OFFSITE STORAGE? CAN YOU ENSURE YOUR INFORMATION IS COMPLETELY PROTECTED AT EVERY STAGE IN THE CHAIN OF CUSTODY?

What would happen if your sensitive records and data were lost during transportation to a storage facility? And what if your customers found out? This checklist outlines everything you need to consider about how your supplier protects your records at every stage – from leaving your possession to secure storage. Use it to assess your chosen supplier's chain of custody processes. Then you can be confident they're able to manage the offsite storage of your information effectively.

TRANSPORTATION

- **Vehicle security** – your supplier's vans and trucks need to be secured with comprehensive, up-to-date security features, such as high-security locks, GPS tracking and an independent alarm.
- **Driver competency** – all drivers should be assessed regularly to ensure their licences are valid and that they're fully trained and able to carry out their tasks.
- **Climate control** – your supplier should be able to maintain an optimal environment for transporting media, with a temperature between 61ºF to 77ºF degrees.
- **Cases and boxes** – your supplier should offer a range of pre-tested cases and boxes that meet your individual needs for transporting information.
- **Escalation processes** – your supplier should have records of all security issues that have been escalated. All drivers should carry mobile phones in case similar issues arise.
- **Electronic signatures** – as pieces of information move through the chain of custody, your supplier should document this with an electronic signature. This will ensure you have an audit trail, which helps you meet compliance requirements.
- **Cross-contamination** – your supplier should have procedures in place to manage any spills or damage to information in transit. If this occurs, they should be able to quarantine information immediately.

PROCESSES AND TECHNOLOGY

Core records management system – your supplier should have a records management system to keep clear details of where your records are throughout every stage of their lifecycle. This information needs to be fully auditable.

User permissions – there should be a secure and straightforward process to add and remove users to your supplier's information management system, and to change individual permissions profiles.

Ease of use – ensure you understand the process for moving information along the chain of custody. Make sure you know how simple it is to schedule pick-ups or request records. Ideally, your supplier should have an online portal to make things easier.

Authorisation – does your supplier have processes in place to ensure the confidentiality and security of your customer records? They should provide you with an agreed list of authorised users, confirmed delivery locations and agreed security protocols.

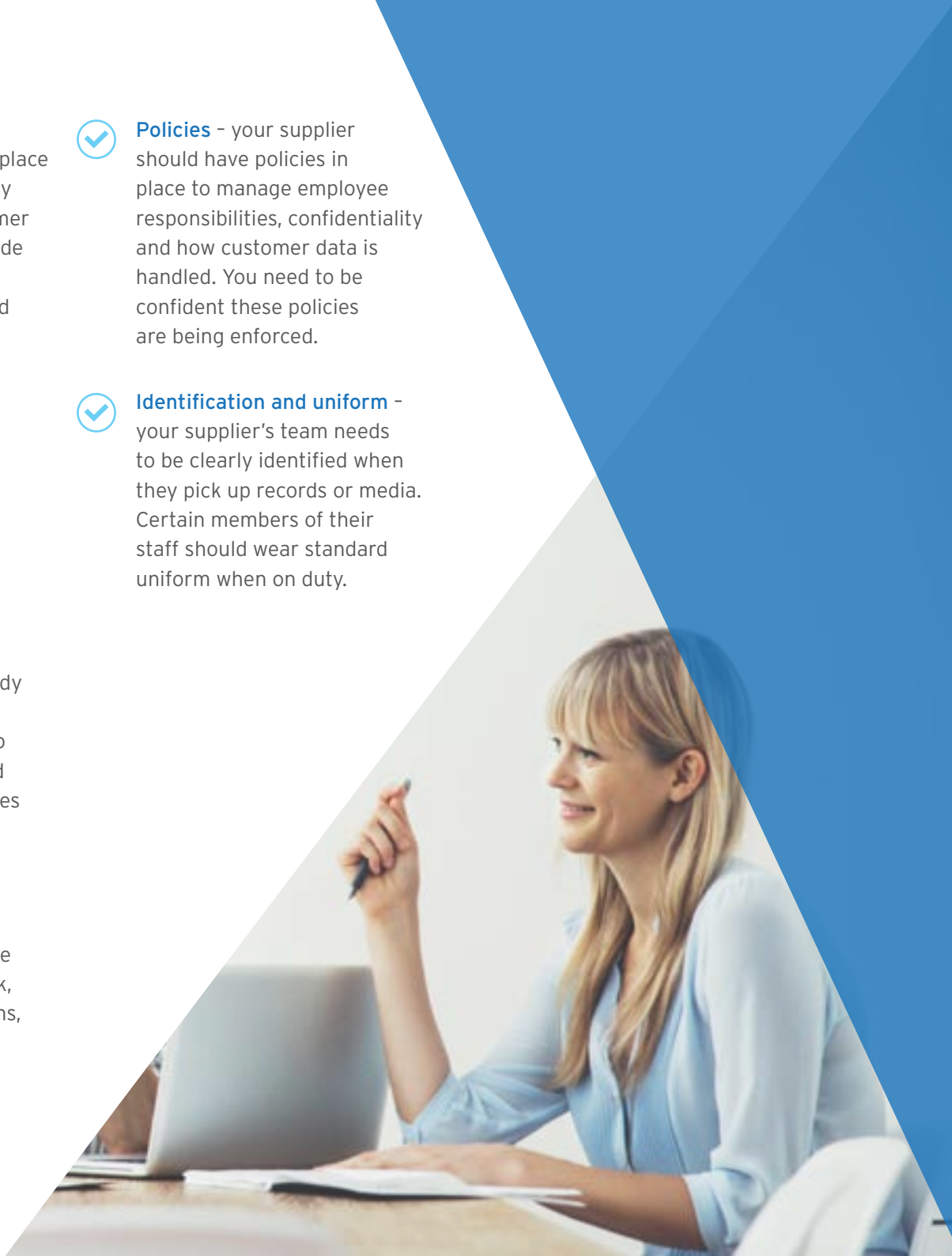
PEOPLE

Training – all of your supplier's staff should be trained to carry out their job functions in a way that conforms to chain-of-custody best practice. For example, drivers should be trained to improve their levels of road safety and to ensure vehicles are never left unsecured.

Background checks – all staff should be properly screened. This could include checking their right to work, identity and global sanctions, and criminal records.

Policies – your supplier should have policies in place to manage employee responsibilities, confidentiality and how customer data is handled. You need to be confident these policies are being enforced.

Identification and uniform – your supplier's team needs to be clearly identified when they pick up records or media. Certain members of their staff should wear standard uniform when on duty.



PHYSICAL SECURITY

Site security – your supplier's facility, including the loading dock, should be protected by a security fence with restricted access gates. All windows and openings should be fitted with shutters.

Surveillance – CCTV cameras should be in operation at all times and regularly monitored and/or recorded.

Access – your supplier should have effective security measures at all entry points e.g. swipe cards. All staff should carry identity cards, and visitors and contractors should be issued with temporary identity cards.

Visitors – all visitors should be checked into the facility. They should be correctly signed-in, documented and escorted at all times.

Audits – your supplier should have processes in place to audit the physical flow of information and documentation in and out of their facility.

Fire prevention – does your supplier have adequate measures in place to prevent fires? Ideally, they should have automatic fire prevention detection and control devices.

Make sure your information management supplier meets your criteria for all the items listed above. That way, you can ensure your sensitive information is effectively protected through every stage of the chain of custody.

FOR MORE INFORMATION ABOUT HOW IRON MOUNTAIN PROVIDES SECURE CHAIN OF CUSTODY FOR INFORMATION MANAGEMENT, CONTACT US TODAY AT +46 8 55 10 2030 A FREE QUOTE ONLINE.

WANT TO LEARN MORE? VIEW OUR CHAIN OF CUSTODY BLUEPRINT DOCUMENT TO LEARN MORE ABOUT OUR FULL SET OF CHAIN-OF-CUSTODY PROCESSES.

CLICK HERE