EMPLOYEE SAFE TRAINING CHECKLIST:

Ensuring Only the Right People Have Access

1. Define Access Roles Clearly

Start by outlining who should have access to the safe and why. Divide roles based on responsibilities:

- Store Manager or Shift Supervisor – Full access, including deposits and code changes.
- Assistant Managers or Team Leads – Limited access based on shift.
- Employees – Deposit-only access in certain models like depository safes.

2. Use Individual Access Codes

Many electronic safes allow for multiple user codes. Assign individual codes to each authorized employee and keep a secure master code for administrative use.

Benefits:

- Tracks who accessed the safe and when (if safe supports audit trail).
- Easy to deactivate one code without affecting others.
- Enhances accountability and minimizes risk.

3. Change Codes Regularly

Even with limited access, codes should be updated:

- After an employee leaves the company.
- If a breach or suspicious activity is suspected.
- As part of a quarterly or semi-annual security protocol.

Make it a routine security practice. Just like changing passwords, rotating safe codes helps reduce long-term vulnerabilities.

4. Limit Keyholder Access

Even with limited access, codes should be updated:

- After an employee leaves the company.
- If a breach or suspicious activity is suspected.
- As part of a quarterly or semi-annual security protocol.

5. Train Employees on Safe Protocols

Security starts with training. Educate your staff on:

- How and when to access the safe.
- What to do if they suspect tampering.
- Why security procedures matter (both for the business and their protection).
- Emergency protocols in case of a robbery or threat.

6. Use Time Delay & Audit Trail Features

If your safe supports it, enable:

- Time-delay features – adds a delay after code entry before the safe opens, deterring robbery.
- Audit trails – tracks code usage, showing who accessed the safe and when.

These features are especially useful in high-risk or high-traffic environments like gas stations or convenience stores.

7. Don't Share Codes or Shortcuts

It may seem convenient to share one code among several employees — but that's where problems begin. Shared access:

- Makes it harder to investigate security breaches.
- Encourages casual behavior toward sensitive access.
- Reduces accountability.

Set the tone that code sharing is against company policy, no matter how trusted the team is.

2707 N. Garey Ave. Pomona, CA 91767 | Tel: 909 445-8888 Toll-free 866 747-7233 | www.bluedotsafes.com