Best Practices in Maintaining the Confidentiality of Customer Materials

This material is intended as security guidelines that a printer uses to protect the confidentiality of its customers' information.

Facilities access

- Visitors to the printing facility should be directed to monitored entrances. Employee entrances should be locked and accessible only via pass code or key card access. Visitors should not be permitted access to production or waste collection areas. Visitors should not be permitted access to printing facilities through loading docks, warehouse doors, or other non-monitored entrances.
- If a visit requires entrance beyond the reception area, guests should be asked to display a visitor's pass that the receptionist or another printing company employee will provide.
- Unless the printer has given written permission in advance, the printer should prohibit use of any type of video or audio recording device on the printer's property, including tape recorders, cell phones that allow for the taking of pictures and/or videos, or video cameras.
- If guests will be entering any production areas, a printing company representative should escort the visitor(s) at all times. Vendor representatives performing technical or contract work for the printer should be escorted to their work area and monitored at regular intervals.
- The printer should post signs noting that access to production areas is restricted.
- A truck driver check-in should exist at each printing facility. Truck drivers should have only restricted access to production areas.

- Unless the facility is fenced and gated in a secure manner, fire doors and other exterior doors that are not monitored should be alarmed when opened or monitored with a surveillance camera.
- Dock doors should be kept closed unless they are in use or unless scissor gates are employed. Scissor gates should be kept closed unless the entryway is in use. Chain link gates should be in place across all exterior warehouse ramps.
- Key railroad and truck dock doors should be equipped with weather shields to limit access while a rail car or trailer is being loaded or unloaded.
- Office areas should be locked at nights and on weekends unless an employee who works in that office is present.
- Printing company facilities should use a surveillance system that includes cameras viewing key access points. Monitors fed by these cameras should be installed in common break areas to help involve all employees in maintaining safety and security. These systems should maintain back up tapes/images.
- Based on specific customer/event requirements, the printing company should retain security guards on-site to supplement the surveillance system.

Access to customer materials

- The printing company should print materials as close as possible to the date on which the materials must be shipped to customer agents or customer-assigned destinations. The printer should print specific events in the most continuous manner possible to minimize the retention of printed work-in-process materials on-site at the printer's facilities.
- No copies of any printed materials produced for the printing company's customers, encompassing items such as sales promotion materials, coupons, rebates, offers, media plans, schedules, samples, art work, data, annual reports, informational mailings, etc., should be allowed out of the printer's facilities prior to

date of sale. These materials should not be removed from the facility for any reason, except as directed by the customer for pick up by, or delivery to, a printing-company-approved outsourced vendor, customer, customer agent(s), or printing company agent(s). The printer's employees and contract personnel working for the printer or in the printer's facilities should be instructed about the confidentiality of the materials they handle. These stakeholders should be prohibited from removing these materials from the printer's premises, except for freight carriers and waste vendors.

- The printer should not share or distribute customer confidential data without prior customer agreement. Contents of the material the printer prepares, prints, or otherwise produces for sales promotion should not be discussed or shared with anyone outside of the company except for a printer-approved outsource vendor, contractor, customer, or customer agent(s).
- Based on specific customer/event requirements, the printing company should use security perimeters, such as temporary walls and roped off areas, around printing presses and allied production areas. When this occurs only printing company employees or contractors directly involved in the production or quality assurance of the job should be permitted access to this area.
- The printer should use state-of-the-art, secure data transfer systems to control the exchange and storage of electronic prepress data. The printer should use firewalls to protect data from unauthorized access.
- The printer should restrict production materials that contain confidential customer information to designated process workflow areas. Employees should be prohibited from removing such materials from those designated areas. Employees should store, file, or put away these materials promptly and in a secure manner upon completion of the tasks.

- The printer's employees should review proofs and printed copies of materials for only production reasons such as verifying content and assuring quality. Access to, and distribution of, these materials should be restricted.

Waste and scrap

- Printed scrap should be shredded, contained, and/or baled prior to recycling or disposal. Such printed waste should be held securely in trailers or other appropriate containers prior to its removal. Other scrap materials containing confidential customer information that are generated in the course of the printer performing services for customers should be disposed of according to the printer's policy. Scrap should not be held; containing, shredding and/or baling should occur as soon as possible after the scrap occurs.
- Based on specific customer/event requirements, the printer should use security guards to monitor complete and consistent containment, shredding and/or baling and disposal of sensitive printed materials.
- The printer should retain all used plates as well as files and any film securely, typically recycling these after the materials date of sale and, in all cases, using processes that restrict access to, and handling of, these materials.
- The printer should securely dispose of and/or shred interoffice paperwork pertaining to confidential customer information.

Skidding and shipping

- The printer should band/wrap printed products slated for distribution on pallets as soon as they are produced for security and protection.
- The printer should release freight loads only to authorized contracted carriers.
- The printer should store banded/wrapped skids of printed materials on-site in secure, restricted areas.

- The printer should not ship store or office copies/non-customer samples with an arrival date that is prior to the date requested by the customer or noted in the print order.
- Access to store and office copies should be restricted to the printer's employees. Based on specific customer/event requirements, store and office copies should be stored in a restricted area. Unused store and office copies should be contained, shredded and/or baled in a secure manner.
- Prior to shipping via UPS, AirBorne, or other third-party carriers, the printer should box or places all products and material into opaque envelopes.

Training and awareness

- The printer's Employee Handbook should outline the requirement of all employees to abide by the printer's policies, including policies pertaining to maintaining the confidentiality of customer materials. The printer should require all employees to sign an acknowledgement that the employee has read, understands, and will abide by these policies.
- The printer should review policies and guidelines pertaining to the maintenance of confidentiality of customer materials with all employees on an annual basis, documenting this review in its Human Resources management system. After the initial review, the printer should require that all employees sign an acknowledgement that they have read and understood this document.
- The printer should require all temporary employees to read, abide by, and acknowledge reading and agreeing to the printer's policies and guidelines pertaining to maintaining the confidentiality of customer materials.
- Every printing facility should post its Policy Guideline on maintaining the confidentiality of customer materials on appropriate bulletin boards in Spanish and in English.

- On a regular basis, the printer's facility managers should formally and informally review the importance of adherence to the printer's Policy Guideline, reinforcing specific guidelines, stressing the importance of maintaining the confidentiality of customer materials, and noting the value that customers attach to the maintenance of the confidentiality of their materials.
- The printer's facility managers should communicate customer confidentiality concerns and expectations with all employees before printing sensitive events.
- The printer should require all third-party vendors and suppliers involved in the production, distribution, or other aspects of the printer's work that may involve customer confidential information receive a copy of the printer's Policy Guideline and a Contractor's Code of Conduct that should also contain a section on confidential information, and/or supplier confidential non-disclosure agreement, and instructs them that their business relationship with the printer is contingent on the vendor's strict adherence to the Policy Guideline and Code of Conduct.
- The printer's position descriptions should include references to the need to keep customer materials confidential. The printer should have a security guard position description on file.

Accountability

- The printer should put into place a policy noting that employees who fail to adhere to the printer's Policy Guideline on maintaining the confidentiality of customer supplied materials, or who fail to report lack of adherence by other employees to these documents, are subject to discipline, termination, and legal action. The policy should communicate to all employees the responsibility and accountability that each employee has with regards to maintaining the confidentiality of customer materials.

- The printer should establish and actively promote a Customer Confidentiality of Materials phone and email hotline to enable anonymous and confidential employee communications with the printing company's management on any actual or perceived breaches associated with maintaining the confidential of customer materials.