

## Assets Protection and Use of Company Resources

Every Lakeland employee is responsible for protecting Lakeland's assets. Lakeland's assets include, but aren't limited to, physical assets, such as equipment and buildings, as well as our funds, and intellectual property such as trade secrets and confidential information.

To protect Lakeland's assets, they must be adequately safeguarded. This means locking up and securing valuable assets where appropriate. Lakeland assets may not be sold, borrowed, lent, disclosed, given away or modified in any way that would impair their value, unless there is a good business reason and with approval of the department manager. Anyone entering a Lakeland or Lakeland-controlled facility is required to wear and openly display a Lakeland-issued identification badge, and follow all entry procedures. All badges are the property of Lakeland and must be returned on termination and upon request.

Each employee is also responsible for understanding Lakeland's obligations for protecting assets that have been entrusted to it by customers or suppliers, and for treating them accordingly.

Company resources, including, but not limited to, cash, personnel, equipment and vehicles can only be used for legitimate company business purposes. Lakeland also provides employees with use of company-owned telephones, copiers and computer equipment to be used as a resource in conducting business. Although reasonable personal use of these resources is permitted, such use is not private, is subject to review and access by Lakeland, and is governed by the professional conduct and reasonable use expectations detailed in Lakeland's E-mail, Internet, Telephone and Computer-use Guideline/Policy.

## Assets

### Information Security

Confidential information generated by or used in any company business activity is considered an information asset. This includes (but is not limited to) information originating from direct access to computer systems, information carried over networks, information preserved on portable electronic media, information appearing in hard-copy format, and other non-public information learned by virtue of being an Lakeland employee.

Lakeland requires that each employee be personally responsible for safeguarding Lakeland's information assets, in all their various forms, from loss, inappropriate modification and disclosure to anyone who lacks either the authorization or the need-to-know. The more sensitive or critical the information, the more care you must exercise in protecting it.

### All employees are required to:

- Correctly classify information assets to accurately reflect their value to our business.
- Protect the confidentiality, integrity, and availability of information such as micro architecture specifications, strategic long-range plans, product pricing, and employee data that, if disclosed, could cause financial or other damage to Lakeland.
- Hold in confidence and not use (except for the benefit of Lakeland) any confidential information that they have access to or that was created by them while employed at Lakeland.
- Employees are responsible to protect confidential information throughout its life, from inception through disposal to ensure confidentiality, integrity, and availability.
- Protect third-party confidential information in the same manner required by the terms of the Corporate Non Disclosure Agreement. If such terms are not known, that information should not be used, copied, or disclosed until the terms of the Corporate Non Disclosure Agreement are known.

- Ensure that confidential information that may need to be released to customers or suppliers is handled properly. In such cases, an employee must have received proper authorization (approval from the general manager or the Legal Department) and must ensure that the recipient has a need-to-know and signs a nondisclosure agreement. Requests for confidential information from outside sources must be handled only by authorized persons.
- Cooperate with Lakeland in protecting such information. This includes, but is not limited to, cooperating fully in any exit interviews, signing a Trade Secrets Acknowledgement Form if asked to do so, and disclosing non confidential information about prospective employment to enable Lakeland to assess any risk to its confidential information.
- Be personally accountable to Lakeland and legally accountable for their actions.

Management and staff are required to maintain an appropriate level of awareness, knowledge, and skill to allow them to minimize the occurrence and severity of information security incidents. Other Information Security Policies (System Managers and Document Control) should be obtained, read, understood and implemented as appropriate.

Each and every employee is required to comply with Information Security Policies and must become familiar with, understand, and follow the Lakeland's Standards and Procedures. Assets.

## **Trademarks and Brands Usage**

Lakeland's trademarks and brands are considered assets of the corporation. Their protection is dependent upon consistent usage and reference. Everyone who is involved in developing communications -- whether Lakeland employees, consultants, outside suppliers or third parties -- is responsible for using Lakeland trademarks and brands properly in both internal and external documents, and in electronic communications.

Lakeland respects the trademarks of third parties and applies the same standards for third-party trademarks. Information, training, and a guide to using trademarks and brands are available through the Lakeland's Legal Department.

## **Assets**

### **Business Continuity**

Lakeland strives to prevent injury to employees, guests and neighbors; protect Lakeland's assets from damage or loss; and minimize the effects of any incident so that they do not compromise Lakeland's ability to achieve its mission. Lakeland recognizes that a wide variety of disasters (natural and human-caused) or failures (physical and information systems) can occur. Although these incidents cannot always be avoided even where preventative measures have been taken, through effective planning we can reduce both the duration and severity of any event that does occur. To accomplish our goals of preventing injury, protecting assets, and minimizing the impact of any incident, Lakeland operations incorporate Business Continuity as a core business practice. Business Continuity is an integral approach to doing business that promotes safety as a core value while providing reasonable assurance we can respond to emergencies and keep our core business running during times of unexpected events or disasters.