BEST PRACTICES
DIGITAL BILLBOARD SECURITY

Maintaining billboard security is important to the outdoor advertising industry as a security compromise impacts the entire industry when it occurs. The following provides best practices for billboard operators to minimize the potential for unauthorized access. Additionally, this document outlines security measures Daktronics has implemented.

HOW TO PROTECT AGAINST OUTSIDER UNAUTHORIZED ACCESS:

PHYSICAL HARDWARE SECURITY

- Install physical deterrents around your display such as fencing
- Install locking device at the access points
- Install security cameras to monitor physical site activity

PASSWORD STRENGTH FOR MODEM, DEVICES USED TO ACCESS DISPLAY CONTROLS AND VISICONN/VENUS SOFTWARE

- Immediately change the default password
- Use at least 12 characters, including upper-case, lower-case, numbers and symbols in no logical order
- Do not use common dictionary terms or predictable word or number patterns
- Implement process for routinely changing passwords *ex. Every 90 days*

HOW TO PROTECT AGAINST INSIDER UNAUTHORIZED ACCESS:

DEVELOP INTERNAL SECURITY PLAN FOR YOUR COMPANY

- Maintain list of everyone who has access to the display

IMPLEMENT PROCEDURE FOR EMPLOYEE STATUS CHANGE

- Employees who are no longer with your company, or move to a position that no longer requires access, should immediately have access removed.
- If your company has keys or pass codes to the display site, ensure those are collected or changed upon employee status change.

DAKTRONICS SECURITY MEASURES

ON-SITE SECURITY

- When unauthorized physical access is detected and reaches a point when there is an ability to add external content. The displays goes blank and Daktronics Network Operations Center (NOC) (for monitored displays) is notified. At this time, Daktronics must be contacted in order to resume scheduled content.
- If unauthorized access occurs, Daktronics billboard displays are equipped with a secondary channel that allows Daktronics to remotely access display power.

CRITICAL SYSTEM COMPONENTS ARE STRATEGICALLY PLACED TO MINIMIZE UNAUTHORIZED PHYSICAL ACCESS.

WHITE LIST

- Only specific IP addresses have access

DAKTRONICS CORPORATE NETWORK SECURITY STATEMENT

Daktronics develops, deploys and maintains an information security architecture that includes security policies, procedures and standards that meet Daktronics business needs. We set forth programs, policies, standards and procedures to create a risk management framework to minimize the risk of compromise within Daktronics and to align with industry standards for risk management.

If you feel you may have been compromised or for security related questions, please contact your Daktronics representative.

201 Daktronics Drive PO Box 5128 Brookings, South Dakota 57006-5128
1-800-DAKTRONICS 800-325-8766 605-692-0200 fax 605-697-4700
www.daktronics.com email sales@daktronics.com
DD3682607 071217

DAKTRONICS