CASINO CRUISELINES
Casino Motorcoach Marketing Programs

SERVING CASINOS ✦ Since 1993

Web Application Assessment Security Policy

For Employees and Contractors
Information Security Team (InfoSec)

Purpose

The purpose of this policy is to define web application security assessments for casino express websites provided by Casino Cruiselines.

Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Casino Cruiselines.

All web application security assessments will be performed by the InfoSecurity Team (InfoSec) which comprises delegated security personnel either employed or contracted by Casino Cruiselines. All findings are considered confidential and are to be distributed to persons on a "need to know" basis only.

Policy

The current approved web application security assessment tools in use which will be used for testing are: GoDaddy SiteLock Website Security Deluxe.

Confidential Information stored on electronic and computing devices whether owned or leased by Casino Cruiselines, the employee or a third party, remains the sole property of Casino Cruiselines and/or its Clients. You must ensure through legal or technical means that Confidential Information is protected.

You have a responsibility to promptly report to the InfoSecurity Team (InfoSec) the theft, loss or unauthorized disclosure of any Confidential Information.

You may access, use or share Confidential Information only to the extent it is authorized by the Chief Information Officer. You may access, use or share Client Confidential Information only to the extent it is authorized (either by that Client or pursuant to any agreement between Casino Cruiselines and that Client) and necessary to fulfill your assigned job duties. You may not request a Client's authorization to disclose any Client Confidential Information without first obtaining permission from the Chief Information Officer.

All users of the Call Center must have unique login credentials.
The login accounts of Call Center users whose employment has been terminated must be disabled within 24 hours.

System level and user level passwords must comply with the Password sections in this policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must he secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log Off when the device is unattended.

Policy Compliance

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee or contractor of Casino Cruiselines authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Casino Cruiselines-owned resources.

The following activities are strictly prohibited, with no exceptions:

Accessing data, a server or an account for any purpose other than conducting Casino Cruiselines business, even if you have authorized access, is prohibited. Introduction Of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Using a Casino Cruiselines computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Providing information about, or lists of, Casino Cruiselines employees or contractors, or any other Confidential Information to parties outside Casino Cruiselines, except as otherwise expressly permitted by this policy.

Password Creation

- All user-level and system-level passwords must conform to the Password Construction Guidelines stated in below.
- Users must not use the same password for "Casino Express" accounts as for other Casino Cruiselines and non- Casino Cruiselines access (for example, personal ISP account, option trading, benefits, and so on).

Password Change

- All Call Center user-level passwords must be changed at least every 90 days.
- Password cracking or guessing may be performed on aperiodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as highly sensitive, Confidential Information of Casino Cruiselines.
- Passwords must not be inserted into email messages or other forms of unsecured electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share Casino Cruiselines passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Any user suspecting that his/her password may have been compromised must report the incident and change his/her passwords.
- You shall maintain logical separation between the Client Confidential Information of each Client and Client Confidential Information of other Clients;
- Database servers may not be accessible remotely (out of network);
- "Client Express" sites must contain a Privacy Policy page that details the use and storage of PII; The Privacy Policy must be approved by the Chief Information Officer.

- “Call Center” application login screen must prominently alert any user, whether authorized or not, of the presence of Confidential Information;
- Applications must support authentication of individual users, not groups;
- Applications must not store passwords in clear text or in any easily reversible form. Database storage shall be encrypted;
- Applications must not transmit passwords in clear text over the network; and Applications must provide for reasonable role management, such that one user can take over the functions Of another where necessary without having to know the other’s password.

Statement of Guidelines

Password Construction Guidelines
All passwords should meet or exceed the following guidelines:

Strong passwords have the following characteristics:

- Contain at least 7 alphanumeric characters.

Contain both upper and lower case letters.

Contain at least one number (for example, 0-9).

Contain at least one special character (for example, !$^&*_+|={}[]:?)

- Poor, or weak, passwords have the following characteristics:

Contain less than eight characters.

- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvutS, or 123321.

Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).

- Are some version of “Welcome123” “Password 123” ‘Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, “This May Be One Way TO Remember” could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

Updated: 6/27/17