Security Best Practices for Artists

Security is the responsibility of all industry professionals

Physical Security

Deny unauthorized access to facilities, equipment and resources. Protect personnel and property from damage or harm.

- Only invite employer authorized visitors into your place of work.
- Never share your work ID badge, access fob or keys with other individuals.
- Keep sensitive physical items like scripts, props and removable storage devices locked in secure storage when not in active use.

Password Security

Minimize risk of unauthorized access to your accounts.

- Never share your password or allow anyone else to use your account, you are responsible for all activity carried out by your user account.
- Periodically change passwords and always use strong passwords for all of your accounts.
- Use different passwords for content access and other services.
- Never send login and password credentials together, share the information via two separate channels, i.e. email the username and text the password.
- Keep passwords secure, never with a device containing content (e.g., a Post-It note on a computer, laptop or encrypted drive is a no-no).

Content Security

Minimize unauthorized access or loss of digital content.

- Only transfer digital content using secure methods approved by your client or place of work, never by email or unencrypted services like FTP.
- Your place of work has a secure network and it is your responsibility to keep it secure by not connecting any unauthorized hardware or installing software without permission.
- Store digital content in the appropriate location to ensure it is backed up regularly.
- Only use cloud storage or backup services such as Google Drive or Dropbox for client content or other sensitive material if you have explicit approval from the client or your employer to do so.

Beware of Social Engineering

The practice of manipulating individuals to involuntarily divulge confidential information. A common tactic.

- Always make sure you read and follow the security policies provided by your client and/or employer. Never share content with people who are not approved by the content owner to receive, handle or view it. Only people who are directly working on a project may have access to such content.
- Professional profiles, such as LinkedIn and IMDB, should never include any information about unreleased projects you have worked on unless you have clearance to do so.
- When possible, always refer to projects using code names rather than the actual title.
- Talking with colleagues about your work in a public place should be done with great care and never within earshot of anyone who does not currently work with you.

Security Incidents

What if you suspect a breach of security?

- Any suspected loss of content should be reported immediately to your employer or the content owner.
- Do not condone security negligence or breaches by others, or “turn a blind eye”; not reporting an incident you are aware of makes you liable too.
- When in doubt, please seek advice from your supervisor or technology team.

Please note: these are **general guidelines** written by the VES Technology Committee. Specific security policies may vary by studio, facility or production.

If you have any doubts or questions, please do not hesitate to ask your producer, supervisor or the HR department of your employer.

For more information see http://www.fightfilmtheft.org/facility-security-program.html