

Web Privacy and Security

Chris Kidd
Chief Information Security and
Privacy Officer

1. Address Third-Party Risks

- If hosting site externally:
 - Ensure U's Security Contract signed
 - Requires reasonable level of security
 - Prohibits use of information for any other purpose

2. Use Strong Passwords

- If easily guessed, your web page could be defaced, or worse, malicious code could be added.
- Eight characters and a mix of upper and lower case letters, and non-alphanumeric characters, too.

Example:

- I Like To Drink Dew = iL2Dd3w!



3. Parental Consent/Safety Considerations

- Collection from children 13 and under, without parental permission, is illegal.
 - How are you checking age?
- If "mature" content, consider adding an Internet Content Rating Association (ICRA) label.



4. Encrypt Sensitive Data

- If collecting sensitive or confidential information:
 - Ensure you are using SSL
 - Consider encrypting stored data
- Do not use self-signed certificates



5. Maintain Logs

- Every time a web page is accessed, you should log at least:
 - IP address of the visitor
 - Date and time of the page request
 - The URL of the requested file
 - The "referrer" url
- Log files should be kept separate from web-server



6. Vulnerability Scanning

- Have your web-site scanned on a routine basis & remediate any vulnerabilities
 - Contact the Help Desk
 - Campus – 1-4000
 - Health Sciences – 1-6000



7. Know Privacy Practices

- University Privacy Notice
- University Health Care Privacy Notice



8. Seek Advice & Report Issues

- Seek advice and/or report any compromises, or potential compromises:
 - <http://www.secureit.utah.edu>
 - 7-9241



Questions?

