

INTERNET AND PUBLIC COMPUTER ACCEPTABLE USE

APPENDIX A-

Brown County Technology Services: Filtering Tool

Brown County Technology Services (BCTS) uses an automated Internet filtering tool on county computers.

The industry-leading Cisco IronPort Web Usage Controls provides visibility and protection from Web acceptable use violations. Its dynamic categorization catches 90% of objectionable content including pornography, adult, hate, and gambling sites.

Tech Summary of how the tool works overall:

https://www.cisco.com/web/about/facts_info/privacy/wuc_09_11_09-external.pdf

Without exception, Cisco blocks child abuse content for all customers and for legal reasons keeps no logs.

Listing of the categories created (dynamically) by the tool:

http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/sc5126/CategoriesAP.pdf

Protection Against URL-Based Threats

An increasingly common characteristic of malware is the presence of a URL that a user must visit to be attacked. Spam, URL-based viruses, phishing attacks, and spyware all direct the user to a malicious URL. Cisco Web Reputation Technology's accurate analysis of these URLs helps:

- Stop attacks much more quickly and accurately
- Avoid the URL in whatever method it is disseminated
- Protect against sophisticated blended threats.

BCTS blocks malicious software sites (sites that would damage the computer software) which may result in legitimate sites being blocked from time to time through this tool.