

CCSIDA-ISF The Implications and Cause-Effect of County Use of Social Networking

This white paper is a result of the ISF Subcommittee on *County Use of Social Networking Sites* roundtable discussions. It contains proposals for best practices as well as for CCSIDA-ISF to develop a 'position publication' adopting a set of basic recommendations for Counties' use of Social Networking Sites.

Whether a county takes advantage of social networking opportunities is a 'risk based' decision. The business case must outweigh the associated risks or the risks must be mitigated to an acceptable level prior to use of social networking sites. When the choice is made to use social media, it must be controlled and wrapped around technology protection schema and policy. And because communication methods are in constant flux, (5 years ago a "tweet" was the sound a bird made), the means by which counties disseminate information and interface with the public will change so those technologies and policies need to be kept current. While social sites are currently the 'hot' way to get a message out, there are some indications that may change in the future.

But, today, the question is: Can we use social networking sites effectively and safely AND within the constraints of county security and privacy considerations and our own risk tolerance?

Benefits

- Allows for many ways to communicate to constituents
- Many constituents are comfortable using social networking sites
- Better access to younger subset of society
- Encouraged by the State of California

Risks associated with Social Networking

- Exposure to County because of bad security habits of users A real life-example: Hacked into County network (E-mail System) by using unchanged User-ID and Password. Result was County 'blacklisted' (multiple times) as a spam sender. VPN access compromised.
- Exposure to County in unanticipated litigation from (unintended) violation of law (which can be a moving target). Example: EU- Google Management in Italy prosecuted for violating EU Privacy Law by allowing a posting to happen containing private/damaging information.
- 'Stale' information remaining on postings could be damaging or open up liability.
- Managing 1st amendment rights violations if allowing replies or 'public conversations' to County postings. Moderating sites can be a Pandora's Box of costly issues...
- Resources to manage both 'outgoing' and 'incoming' (budget constraints) and who's going to 'police' (and pay for that person)?
- Reputational Risks (individuals and County).
- Liability on not reacting to a threat posted on a County page.... reasonable diligence, expected protections... should have known that threat could result in injury...
- Exposure to leak of confidential/sensitive data.
- Instead of just 'watching' and managing just one site (county Web Pages), now there's many different sites, different operational processes...
- Increased risk of 'social engineering' (and 'spear' phishing).
- Increased risk of malware into County.

- o Increases risks of re-direct efforts to 'official looking' sites that are unauthorized.
- o Additional temptation for staff's attention to be diverted to non-County Business.
- o Backups/Archive/PRA's/eDiscovery impacts This is the White House page on Facebook. Comments posted on and messages received through White House pages are subject to the Presidential Records Act and may be archived. Learn more at WhiteHouse.gov/privacy
- o Is site used considered a vendor preference- endorsement by the county? Would it require competitive bids and how? (After all, we are government!)

What we didn't consider (but may need to)

- o If encouraged and used, what's the impact to productivity (Staff usage)?
- o Impact to bandwidth?

Recommendations

- Very strong awareness program addressing social networking use pitfalls for employees at work AND at home (users are and will continue to be the 'weakest link' in protecting County technology assets). Training should cover such topics as:
 - Social engineering
 - Phishing
 - Re-directs
 - Importance of using different (from work) user-id and password to access social networking sites
 - Potential for individual liability
- Encourage social networking sites as **outbound tools only** and lock out the inbound permissions.
- Ensure that what you post on your Web page is the same message as your social networking site(s). Advantages include:
 - Better ability to keep information 'fresh' because as you update your Web Site, you also systematically update your social networking site(s)
 - You still get your word out! (H1N1, specific messages to younger subset of society)
- Permit only authorized personnel to make comments (restrict use of comment moderation and monitoring tools). Consider using a generic County E-mail address for E-mail only contact with a short or 'once read destroy' retention policy. Advantages include:
 - Minimizes e-discovery costs
 - Precludes 1st Amendment Rights management issues
 - Minimizes costs associated with PRA requests
 - Minimizes storage management/backup costs
- Permit Departments to manage their posting, but in compliance with County policy and security/privacy policies. County Public Information Officer (PIO) should be involved. Watch out for copyright infringement and posting liability issues (same as for a Web page).

- Implement heightened IT/Security best practices considering social media website security issues including input validation, code security reviews, and strong cookie management as well as enhancing network and DNS security controls to meet growing risks.
- Discourage 'professional group' relationships for County benefit on social networking sites.
- Prohibit Elected Officials from establishing their own 'personal' Social Networking presence under the County 'umbrella' because they will likely want to allow full constituency interaction. Could also be considered a conflict of interest.
- Develop a Social Networking user security checklist that all assigned and authorized users can follow to help insure that 'best practices' are followed. Take that same 'theme' in developing a 'best practices' checklist for your IT department in developing and setting up social network partnerships with implemented security and privacy processes.

CCISDA ISF offers the following recommendations as best practices to be incorporated into counties' Policy on Social Networking (Media) models...

Counties should encourage the use of social networking sites as an additional means to get important information (highly important or emergency information, not routine...) out to those who are less likely to visit the county's posted web site.

Develop an 'official retention policy' that says that content is retained until posting has been removed and destroyed unless required by law (litigation or potential litigation, existing PRA requests). Coordination with County Counsel and Risk Management is advisable.

Permit one way or outbound only and prohibit public comment. Use designated E-mail for the public to contact a generic E-mail box that is maintained pursuant to your county's normal E-mail retention and destruction policy.

Provide links back to County web sites for information postings or for additional event or pertinent information.

Require Departments to follow all security and privacy policies published by County as well as existing local, state or federal rules and regulations.

Use disclaimers where appropriate. For example: 'the user of this Social Networking site is no longer on a County managed location but on a private, un-regulated site with different privacy policies.' Those authorized to manage social networking sites are subject to county's 'Computer Use Policy'.

Consult with County Counsel regarding maintaining Government neutrality and compliance with applicable statutes.

County departments wishing to use social media sites should be granted specific privileges and responsibilities, including:

- o Limitations on permitted sites
- o Limit access to a small select authorized group of users
- o Maintain specific departmental policy that's consistent County-wide

Follow available 'best practice' security 'hardened' for the use of Social Networking and its associated risks.

Note: After reviewing Sonoma, Riverside, and San Mateo Counties' pending or implemented policies as well as policies from outside the State of California (some have more relaxed PRA's and other rules and regulations) the above represents minimum level of policy practices that this committee feels must be included in the framework of a CCISDA-ISF supported Social Networking/Media Use Policy.

Many Thanks for the invested time of these ISF Members making up our Committee:

Dr. Lisa Scott-Lee, Sacramento

Joe Galvan, Sonoma

Jo Burnett, Sonoma

Stormy Maddux, San Mateo

Russell Rapp, Ventura

Dave Fry, Contra Costa

Robert Pittman, Los Angeles

Greg Bown, Napa

Kent Yeargin, Sutter

Cheri Huber, Napa

Gary Coverdale, Napa