Contact Information

Neighborhood Council: Mar Vista Community Council
Name: mary hruska
Phone Number: 3104032741
Email: mary.hruska@marvista.org
The Board approved this CIS by a vote of: Yea(15) Nay(0) Abstain(0) Ineligible(0) Recusal(0)
Date of NC Board Action: 12/08/2020
Type of NC Board Action: Against

Impact Information

Date: 12/16/2020
Update to a Previous Input: No
Directed To: Board of Neighborhood Commissioners
Council File Number:
Agenda Date: 12/01/2020
Item Number: 12-Digital Media Policy
Summary: The Los Angeles Board of Neighborhood Commissioners (BONC) has provided a draft for a Digital Communications Policy for Neighborhood Councils and has solicited comments from Neighborhood Councils (NCs) prior to passage by the commission. The draft policy includes some good best practices for the use of Digital Communications by Neighborhood Councils (NCs). However, it also contains high risk digital content and credentials management processes that would lay the City and Neighborhood Councils (NCs) open to a variety of cyber and other types of attack. The approaches described in the draft do not follow industry best practices. Therefore, the Mar Vista Community Council opposes passage of the draft Digital Communications Policy for Neighborhood Councils until it is updated to address specific security concerns. Section by section issues with the draft policy (and potential updates) are provided in the Attachment A.

MVCC Community Impact Statement
Board of Neighborhood Commissioners Digital Communications Policy (draft 9-29-20)

Attachment A

MVCC Comments
Draft Communications Policy for Neighborhood Councils (draft 9-29-20)

Section 2.4 Suspension of Accounts
Issue: DONE suspension of an NC's Digital Media accounts (for policy enforcement) is not technically possible with credential management as described (Section 6 and 11). Note that different media platforms have different trust authorities.

Recommendation: Revise wording based on *credential management* options chosen (see comments on Section 6 and Section 11), so that Department policy is enforceable.

Section 4.6/4.7/5 Proposed Account Administrator and Account Moderator Roles
Issue: Two new roles are created for NCs- the *Account Administrator* and the *Account Moderator*. As described, there are a number of issues with these roles:

- Section 4.6-7 describes these roles as plural (i.e., Administrators, Moderators). According to *least-privilege* security, NC digital accounts should be held by, at most, two individuals—the Chair and one designee. The further credentials are dispersed, the more risk to the NC. New roles should **not** be defined that result in proliferation of credentialed users.
- Section 5.3-4 Account Administrator- As above, to maintain least-privilege a new role should **not** be defined. Also, there is confusion in the role description as to whether this is a compliance role (i.e., Chair responsibility) or content creation/management role (i.e., typically communications/outreach chair). It is hard to imagine an NC organization where all of the assigned responsibilities would be performed by a single individual (unless the Chair does all communications/outreach).
- Section 5.5-6 Account Moderator- As above, to maintain least-privilege a new role should **not** be defined. Assigned Moderator responsibilities largely overlap and seem to duplicate Account Administrator responsibilities (e.g., maintain content, ensure quality, manage compliance). Between the two roles, it is not clear whether these are hands-on (i.e., "you do these things") or management (i.e., "make sure these things happen") responsibilities.

Recommendation: Remove Account Manager and Account Moderator Role from Terms in Sections 4.6-7 and 5. Revise Section 5 to clearly state Chair's Digital Communications responsibilities (i.e., policy compliance and quality oversight). Revise Section 5 to clearly state Digital Communications administrator responsibilities (e.g., platform management, postings) to Chair of the committee responsible for communications/outreach.

Section 6.1 Setting up NC Media Accounts

Issue: All media accounts require personal or "fictitious" for initial setup. So noted exception would be the norm.

Recommendation: Two potential options a) DONE sets up accounts on behalf of NCs (similar to what is done for ZOOM and NextDoor), or b) allow NCs to set up accounts based on personal or "fictitious" accounts to be passed to the next corresponding Chairs.

******** Section 6.2 Credential Management and Exchange for NCs *********

Issue: MVCC has spent significant time since July 2019 implementing clean credential management for all media platforms with good account custody practices. The MVCC fully understands that other NCs have had similar problems with lost accounts/passwords, etc., and other NCs have sought assistance from the City to address ongoing account management issues. Unfortunately, the BONC proposed solution to this problem is the MANUAL exchange of password/account information (via unsecured email or phone) from NCs to the City on an ongoing basis going forward. No chain-of-custody of the credentials is described for the NCs, in transit to the City, on City systems and documents. It is well-known that the manual exchange of credentials is fraught with human error, not current when you need it, open to many cyber threats including insider attacks and man-in-the-middle, is how NCs have been functioning, and simply does not work. This change would open MVCC credentials and accounts to possible compromise, with potential liability of the City to resulting impacts. In contrast, current industry best practice for credentials is to utilize one of the many enterprise credential account products and/or services that provide for the secure storage and exchange of credentials. If the City is going to require that they have access to MVCC digital media accounts credentials, *it MUST be implemented ONLY through one of the certified credential services as is currently used by the MVCC.*

Recommendation: Update to referenced approved best practice credential management process (NOT via unsecured email or phone). Three potential credential management solutions are possible.

1) *City provides a Cloud-based industry standard credential management system*
   In this case, a hierarchy would be implemented. Each NC would upload and have access to their credentials and DONE would have access to all NCs credentials on an ongoing basis. The City likely already utilizes such a system that could be made available for use by DONE and the NCs. If implemented, root-account access (by DONE) should only be via MFA (multi-factor authentication), such as a password plus a secure-ID token.
2) *DONE creates accounts and distributes credentials to NCs*
   Similar to what has been done for ZOOM and NextDoor accounts. This solves the problem of DONE having credentials, but adds DONE admin tasks, and adds significant credential transit and custody risk. Also, could be problematic for many different account type setups, since NCs use a variety of Website providers, etc. Significant setup time for the City.

3) *DONE provides training/instructions to NCs to create and securely store their own account credentials*
   MVCC has setup a process for secure credential management storage using no-cost options. This could be duplicated for other NCs. MVCC could provide detailed information regarding current practices to assist in training other NCs.

Section 11 Security and Privacy

Issue: 11.1 is specific to Account Administrator to protect credentials. Should be generalized to ALL NC account holders. Also, not executable without proper tools (e.g. free password management software).

Recommendation: Revise wording to generalize for all account holders. DONE should separately provide recommended password safeguard tools. MVCC has used tools they can recommend.

Issue: 11.3 states that Account Administrator should be "judicious in 3rd party applications." Should be ALL account holders. Refers to "official devices." NCs have no "official devices." "3rd party application" are not described, and this is probably not realistic since NCs will use personal devices.

Recommendation: Revise wording to generalize for all account holders. Clarify what is meant by "3rd party applications."

Issue: 11.4 states that passwords should be different for each account. This is best security practice, but feasible only if credential management systems are in place (see 6.2 comments).

Recommendation: Add, that having separate passwords will be enabled by City-approved password management tools.

Issue: 11.5 states "regularly changed and recorded" for passwords is **not** secure unless saved/retrieved from credential management systems.

Recommendation: Add, that this will be enabled by City-approved password management tools. Also, remove Account Administrator role and generalize to account holder.

Issue: 11.6 Account Administrator role should be removed. Should be generalized to account holder.

Recommendation: Generalize to apply to account holder.

Issue: 11.7 **Credentials (passwords, account information) should NEVER be stored "online, hard disk, or physical space."** Credentials should only be stored in a secure credential management system (many available at no cost).

Recommendation: State that passwords, accounts, and login information must be stored in a City-approved credential management system.

Note that members of other NCs have also identified these and other issues with the draft Digital Communications Policy.

Contact Information
Neighborhood Council: Mar Vista Community Council
Name: mary hruska
Phone Number: 3104032741
Email: busdisora@aol.com
The Board approved this CIS by a vote of: Yea(12) Nay(0) Abstain(0) Ineligible(0) Recusal(0)
Date of NC Board Action: 12/08/2020
Type of NC Board Action: For if Amended

Impact Information
Date: 01/04/2021
Update to a Previous Input: No
Directed To: City Council and Committees
Council File Number: 20-0147-S19
Agenda Date:
Item Number:
Summary: Whereas the Mayor of Los Angeles on March 15 and 17, 2020, signed emergency orders placing a moratorium on evictions due to the COVID-19 crisis until February 1st, 2021, and for rental units covered under rent stabilization ordinances (RSO) until 60 days after the expiration of the moratorium, April 1st, 2021, And Whereas the County of Los Angeles Department of Public Health issued a targeted and temporary Safer-at-Home order lasting from November 30th until December 20th due to new COVID-19 cases in the county begin to exceed a five-day average of 4,500 newly diagnosed cases as of November 27th, And Whereas unemployment in the City of Los Angeles was at 12 percent as of October 2020, compared to 7.7 percent in October 2019, And Whereas the industries that continue to struggle to recover jobs in the City are largely those that pay the lowest wages, And Whereas 57.2 percent of City of Los Angeles residents were considered rent burdened (paying 30 percent or more of their income in rent) as of 2019, And Whereas the California Policy Lab predicts that 750,000 Californians will likely lose unemployment insurance as of December 26th, 2020, if certain provisions of the CARES Act are not extended, And Whereas thousands of Los Angeles families are facing food insecurity, which indicates that these families are likely extremely challenged to cover even basic expenses (i.e. rent or mortgage costs), Therefore, be it resolved that the Mar Vista Community Council Board of Directors requests Councilmembers Bonin and Koretz immediately introduce an ordinance to extend the eviction moratorium in the City of Los Angeles until June 30th, 2021. Therefore, be it further resolved that the Mar Vista Community Council Board of Directors urges that this ordinance be passed before the Winter Holiday Recess.