Committee Topics placeholder page

IDEA: New CCB network to support unsupported devices and networking arrangements

- IT support to CCB theorists and other researchers

What does CCB need to do regarding Nov 2015's Revisions to University Policy 5.10, Information Security?

From: William Dichtel
Sent: Monday, November 30, 2015 10:27 AM
To: Oliver B. Habicht <oh10>; Michael S. Lenetsky <msl37>; William Dichtel <wdichtel>
Cc: Frank L. Strickland <fls1>
Subject: Re: Revisions to University Policy 5.10, Information Security

Hi Oliver,

Thanks for bringing this to my attention. I need a layperson's version of what things we need to do differently within the department regarding this policy.

Thanks,

-Will

From: "Oliver B. Habicht" <oh10>
Date: Wednesday, November 25, 2015 at 2:01 PM
To: "Michael S. Lenetsky" <msl37>, William Dichtel <wdichtel>
Cc: Frank Strickland <fls1>
Subject: FW: Revisions to University Policy 5.10, Information Security

Michael and Will,

There are recent changes to CU's IT Policy you should be aware of, as outlined below.

I intend us in ChemIT to work in coordination with Frank Strickland and the CCB Computing Cmt to help ensure that Chemistry's IT environment takes into account these changes to policy over time. I welcome you input on process, or if you foresee concerns.

Thank you, -Oliver.

From On Behalf Of Cornell University Policy Office
Sent: Wednesday, November 25, 2015 11:21 AM
To: UNIVERSITYPOLICIES-L; PAG-L; EPRG-L
Cc: Wyman Miles
Subject: Revisions to University Policy 5.10, Information Security

Good morning,

The University Policy Office (UPO) announces the issuance of a revised **University Policy 5.10, Information Security**. This revision does not change the substantive philosophy of this important policy, but adjusts certain procedures to adapt to the changing security landscape. Below is a list of the major revisions to this policy:

- a new requirement for whole-disk encryption for all university-owned desktops, laptops, tablets, and smartphones (our best defense against a data breach caused by a stolen device);
- an encryption requirement for removable media on systems that store or process Level 1 data (sharper clarification of an existing requirement);
- the requirement for custom-developed web applications to scan free of vulnerabilities before going live (this is also a request from an old Audit finding);
- the requirement for 2-factor authentication for access to Level 1 data (an old recommendation in the policy now changes to a requirement);
- the recommendation of application whitelisting instead of antivirus on servers hosting confidential data;
- the strengthening of opening statements of Baseline requirements to accommodate growing university use of outsourced solutions.

Please familiarize yourself with this revised policy as it pertains to you, which is available at https://www.dfa.cornell.edu/tools-library/policies/information-security, and direct any questions about this policy to <it-policies>.

Joshua Adams

Director, Cornell University Policy Office and

DFA Communications