Information Security Policy for Users (Not Auditors)

SESSION ID: GRC-W04A

Michael Scheu

Information Security Specialist
D+H

User (AND Auditor) Friendly Information Security Policy

SESSION ID: GRC-W04A

Michael Scheu

Information Security Specialist
D+H

User Impact

- No one will read your 100+ page policy (not even you)

□ I have read and agree to the Terms & Conditions.

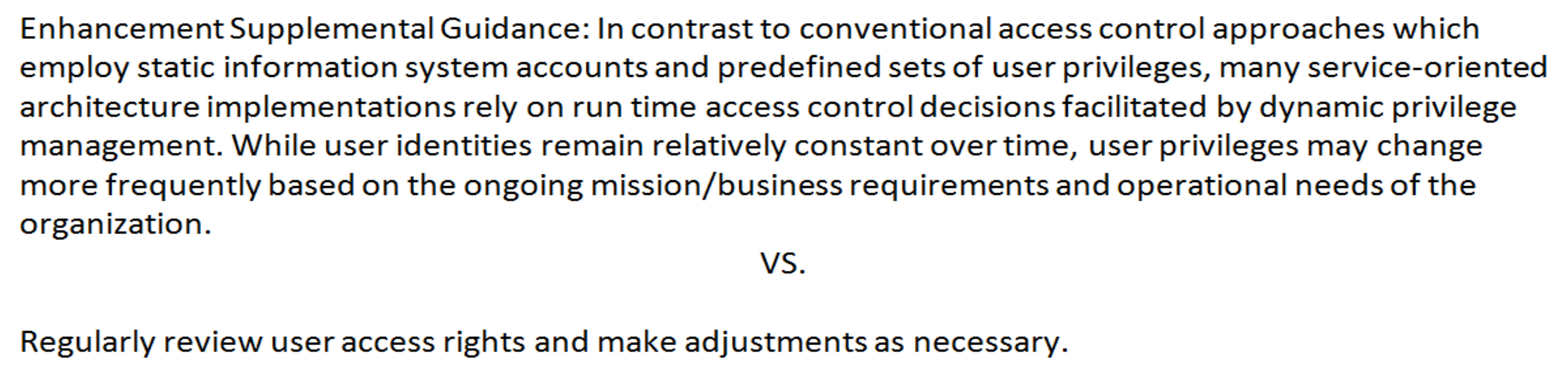
- A huge legalistic policy is not user friendly
- Users need to understand and embrace policy
- A user friendly policy makes for a user friendly InfoSec Department

Challenges

- Lawyers have to consider every contingency (users don’t)
- Policies have to be written so that a user will understand
- Everyone in your company really needs to know the policy
- Auditors will require some topics
- You already have an approved policy

Policy for the Users!

- Consider your audience
- Segregate policies
- Remove procedures
- Use natural language



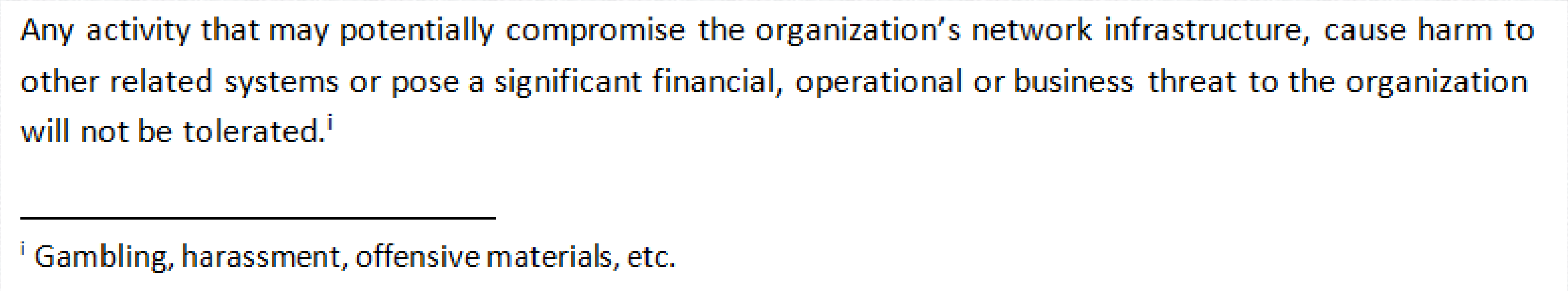
Enhancement Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, many service-oriented architecture implementations rely on run time access control decisions facilitated by dynamic privilege management. While user identities remain relatively constant over time, user privileges may change more frequently based on the ongoing mission/business requirements and operational needs of the organization.

VS.

Regularly review user access rights and make adjustments as necessary.

Policy for the Auditors

- Use footnotes and appendices



Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization will not be tolerated.[i]

[i] Gambling, harassment, offensive materials, etc.

- Keep your required policies, but segregate what Users need from what Auditors need

Goal

- Address the needs of Users
  - Concise
  - Applicable to all users
  - Easily understandable
- Address the needs of Auditors
  - Cover all subjects required by GRC
  - Detailed where needed

Thank You

Michael Scheu

Information Security Specialist for D+H

Michael.scheu@mortgagebot.com