Privacy Filters

Visual Privacy Readiness Checklist

This checklist presents several critical areas of visual privacy protection that should be considered as part of an overall information security strategy. These items fall into three areas: Education, Policy, and Controls.

Education:

- Educational modules on visual privacy included in security awareness training
- Visual privacy awareness education included in new employee orientation
- Specialized visual privacy awareness training for senior managers and at-risk employees

Policy:

- At-risk employees identified along the following criteria
    - Frequency of travel
    - Sensitivity of data managed
    - Time spent working outside the office
    - Regulatory demands on the data accessed/processed
    - Level within the organization – senior management can be particularly at-risk given the "trade secret" or "company confidential" information managed.
- Policies set for at-risk employees
    - Require a privacy filter when working outside the office
    - In severe cases, limit work in high-exposure environments
- Application security policies for visual privacy
    - Applications should mask high-risk data to onlookers. Some strategies - from most secure to least secure - are listed below:
        - Masking of data along with hiding data length
        - "No exposure" character-by-character masking
        - "Brief exposure" character-by-character masking (popular on mobile devices to ensure accuracy of the data typed in a password field for example)
        - Masking a data field only when the field is inactive

Controls:

- Privacy filters supplied to at-risk employees for laptops
- Privacy screen protectors supplied to at-risk employees for tablets, smart phones, and other mobile devices that can access sensitive corporate information
- Privacy filters for mobile workers accessing information outside of the office (e.g. airplanes, trains, coffee shops, etc.)
- Set timeouts on laptop/desktop displays appropriately