UF IT Standards for Data Use Limitations of UF Personally Identifiable Information

UF UNIVERSITY of FLORIDA

Authority

This standard was enacted by the UF Senior Vice President for Administration and the UF Interim Chief Information Officer on July 10, 2008 [5]. It was approved by the UF Chief Privacy Officer and UF General Counsel.

What Constitutes Personally Identifiable Information?

Information used for identification is protected by law [1]. UF calls this UF Personally Identifiable Information (UF-PII). These limitations apply only to personal data covered under Florida Statute 817.5681. Criminal penalties exist for misuse of other personal information [4]. UF requirements for protecting credit card information are covered in a different standard [3].

UF-PII is name together with one or more of the following:

- Social security number
- Driver license number
- Financial account number in combination with any security code, access code, or password.

Limitations of UF-PII Use:

1. Storage on and transmission between servers and desktops managed by UF IT Workers is permitted only for authorized roles. Encryption is recommended.
2. Storage on backup media is permitted only for authorized roles. Strong encryption is required for easily portable backup media. A backup policy must be documented that minimizes retention and specifies destruction of obsolete data.
3. Storage on personally managed computers, portable computers, and removable media requires approval by the UF Privacy Office, even for authorized roles, and should be very rare. Where such usage is unavoidable, strong encryption is required.
4. Transmission involving non-UF servers and networks should be avoided and needs approval by the UF Privacy Office, even for authorized roles. Encryption is required.
5. Anyone with access to UF-PII must attend UF-sanctioned data protection training and must agree to comply with UF data protection requirements.
6. Removal of UF-PII from UF premises requires approval by the UF Privacy Office [2].
7. Any alternatives or exceptions to these limitations must be approved by the UF Privacy Office. They should be rare and they must be documented.

Bibliography

[1] Florida Statute 817.5681, Breach of security concerning confidential personal information in third-party possession; administrative penalties: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC5681.HTM&Title=-%3E2006-%3ECh0817-%3ESection%205681#0817.5681

[2] UF Privacy Policy: http://privacy.ufl.edu/

[3] UF IT Standards for Restricted Data Use Limitations of Financial Account Information: http://www.it.ufl.edu/policies/security/drafts/fai.pdf

[4]Florida Statute 817.568, Criminal Use of Personal Identification Information: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC568.HTM&Title=-%3E2007-%3ECh0817-%3ESection%20568#0817.568

[5] DDD announcement of this standard, http://lists.ufl.edu/cgi-bin/wa?A2=ind08&L=DDD-L&P=R35323&I=-3