

| Classification Levels | | Typical Data Retention Durations | | Data Security Controls | |
|----------------------------|----------------------|----------------------------------|-------------|------------------------|-----------------------------|
| Military Sector | Private Sector | Business documents | 7 years | Data in Use | Scoping & tailoring |
| Top Secret | Sensitive | Invoices | 5 years | | |
| Secret | Confidential | Accounts Payable / Receivable | 7 years | Data at Rest | Encryption |
| Confidential | Private | Human Resources - Hired | 7 years | | |
| Sensitive but unclassified | Company restricted | Human Resources - Unhired | 3 years | Data in Motion | Secure protocols e.g. https |
| | Company confidential | Tax records | 4 years | | |
| Unclassified | Public | Legal correspondence | Permanently | | |

| Data Ownership | | | | |
|--|---|-------------------------|------------------------------------|--|
| Data Ownership | Data Custodian | Systems Owners | Administrators | End User |
| Top level/Primary responsibility for data Define level of classification Define controls for levels of classification Define baseline security standards Impact analysis Decide when to destroy information | Grant permissions on daily basis Ensure compliance with data policy and data ownership guidelines Ensure accessibility, maintain and monitor security Data archive Data documentation Take regular backups , restore to check validations Ensure CIA Conduct user authorization Implement security controls | Apply Security Controls | Grant permission for data handling | Uses information for their job / tasks Adhere to security policies and guidelines |

| Data Classification Criteria |
|--|
| Value - Usefulness - Age - Association |
| Data Retention Policies |
| The State of Florida Electronic Records and Records Management Practices, 2010 The European Documents Retention Guide, 2012 |

| Data Remanence | |
|----------------|---|
| Sanitizing | Series of processes that removes data, completely |
| Degaussing | Erase form magnetic tapes etc to ensure not recoverable |
| Erasing | Deletion of files or media |
| Overwriting | Writing over files, shredding |
| Zero fill | Overwrite all data on drives with zeros |
| Destruction | Physical destruction of data hardware device |
| Encryption | Make data unreadable without special keys or algorithm |

| Security Policies, Standards & Guidelines | |
|---|---|
| Regulatory | Required by law and industrial standards |
| Advisory | Not compulsory, but advisable |
| Informative | As guidance to others |
| Information Policy | Define best practices for information handling and usage -Security policies: Technical details of the policies i.e. SYSTEM security policy: lists hardware / software in use and steps for using policies |
| Standards | Define usage levels |
| Guidelines | Non-compulsory standards |
| Procedures | Steps for carrying out tasls and policies |
| Baseline | Minimum level of security |

| Standards | |
|--------------------|---|
| NIST | National Institute of Standards Technology |
| NIST SP 800 Series | Computer security in a variety of areas |
| 800-14 NIST SP | Securing Information Technology systems |
| 800-18 NIST | Develop security plans |
| 800-27 NIST SP | Baseline for achieving security |
| 800-88 NIST | Guidelines for sanitation and disposition, prevents data remanence |
| 800-137 | Continuous monitoring program: define, establish, implement, analyze and report |
| 800-145 | Cloud computing standards |
| FIPS | Federal Information Processing Standards |