Information Security Policy Blueprint

Records inventory

Risk assessment of data

Data encryption

- At rest
- In transit
- On devices

Access controls

- Physical space:
  - Who is allowed where in the office space and when
  - Recording all access

- Firm data:
  - Inventory of all file and folder access
  - Who in the firm has access to what data
  - Managing that access (who really needs access to it and do they still need access today?)
    An approval process for when access changes
  - An annual review of the inventory
  - Logging of all access
  - Reporting of daily changes
  - Reporting of failed access attempts
    - Is it an accident of is someone methodically looking for something?

- Disposal of
  - Digital data
  - Mobile devices
  - Desktops and laptops
  - Fax and copy machines
  - Memory sticks
  - Disks

- Permitted use of the firm's systems and networks

Onboarding/Off-boarding

- Standards of access to firm systems, data and devices
- Training – from Welcome to the firm, to information security, to here is how to use firm systems

Remote access

Permitted use, when, where and when not to use it

Offsite storage

- Recordkeeping, when items go in and when they come out
- Who can authorize it
- Multiple layers of approval

Cybersecurity

- Firewalls
- Malware/anti-virus
- Intrusion detection
- Monitoring and alerting

Incident response

- What to do when certain incidents happen
- Who is involved
- Who communicates
- Investigative steps
- Remediation steps
- Law enforcement notification
- Regulatory notification

Backup and restoration

- How often
- How many copies
- Retention policies
- Who can request a restoration
- How fast can restoration occur
- What is the priority order on a restoration

Network segregation

- Breaking the network up into segments so as to limit overall network outages and to slow down anyone who may breach the network

Vendor management, including cyber protection

- Cyber Due Diligence Questionnaire
- What vendors must complete the DDQ
- How often are DDQs updated
- How are DDQs verified

Business continuity plan

- Testing
- Documentation
- Business plans for when the office, data center, city, town or state is down

Physical inventory

- Acquisition
  - Who is allowed to purchase what
  - Tagging of inventory
- Disposal and shredding
  - Certificates that this has been done

Application inventory

- Purchased
  - License and contract terms
  - Software code in escrow in the event the manufacturer goes out of business
  - Who has permission to use
  - Version control and update records

- Developed in-house
  - Inventory management control
  - Checking software out and back in by developers
  - Tracking all changes
  - Version control

Information Systems

- Acceptable use policy
- Privacy
  - Who owns what on company systems
  - Users waive any expectation of, or right to, privacy
- Use for business only
- Make it consistent with all firm policies
- Business-related data is stored on firm network
- Limit use of any personal data
  - Reinforce that *anything* on the firm network may be reviewed by the firm
- Cloud storage
  - Firm storage only
  - No access to private cloud storage because of data loss concerns
- Abide by laws and regulations with various software and systems used
- Prohibited activities
  - Public chat rooms
  - Hacking

Message retention

- E-mail
- Instant messages
- Text messages

Authorization

Testing and certification