**Information Security Exception Management - Process Flow Overview**

**Initiation**
- Contact / Request for Exception
- Open Ticket
- Consult / Clarify Request
- Acknowledge Request

**Evaluation**
- Develop Initial Risk Assessment
- Notify Stakeholders, Privacy Officer, Card Compliance

**Approval**
- Document Approval
- Risk Level: Approved, Disapproved
- Implement any Compensating Controls
- Notify Stakeholders of Disapproval

**Monitoring & Review**
- Reporting

**Artifacts**
- Information Security Policy
- Exception Form (Optional)
- Security Architect
- Compensating Control Plan (Optional)
- Level of Risk Notified

**List of Approvers by Department**
- Departmental: (ex. IT Director, Service Owner, College Dean or Administrative Head)
- Stakeholder: Administrative Procedure specific

**Supervisors & Approvers**
- CISO Approval
- University VP of IT Approval
- Compliance Approval
- IT Approval

**Status**
- Open
- Assigned
- Notified
- Evaluation / Stalled
- Department Approval
- Compliance Approval
- IT Approval
- Approved / Disapproved
- Closed

**Monitoring and Reporting**
- Schedule Follow-up and/or Review
- Reporting

**Due Diligence**
- Ensure Risk
- Develop / Update Compensating Control Plan
- Document Final Risk

**Policy**
- University of Minnesota – Information Security Exception Management

---

Departmental options include: IT Director, Service Owner, College Dean, Administrative Head, Dean, Departmental lead users.

Administrative options include: CISO Overall, Privacy Officer, Card Compliance.