Théophane Paradis

Principles :

- **Of Least privilege**
  Why : if a simple user has administrators level access rights and permissions, anyone can go in the network and destroy it or just to use it to what he wants.
  Control : ring 0 (one ring to rule them all) / Protection ring
  Example of successful attack : SNMP (Single Network Management protocole exploitation) (Layer 7 - Application). Attackers abuse over-permissive configurations to control network devices.
  Security measure / strategy : Limit permissions strictly to necessary functions.

- **Segregation of Duties**
  Why : Limit the scope of action of a compromised target, the scope of damage too.
  Control : Unix file system permissions → separate roles and control file access.
  Example of successful attack : VLAN hopping (Layer 2) – used to go on isolated network segments.
  Security measure / strategy : Enable ID VLAN filtering and disable DTP (Dynamic Turking Protocol).

- **Complete mediation**
  Why : Access request ← must be verified to prevent privilege escalation.
  Control : sudo word ← got only the right for certain tasks (only been granted to have root access to the specific executable / path). It ensures a minimal access.
  Example of successful attack : HTTP Parameter Pollution attacks (Layer 7). Attackers manipulate unmediated requests to escalate privileges
  Security measure / strategy : Enforce strict access controls for each request.

- **Acceptabiliy**
  Why : if a security solution requires to many effort, if it is to costly, a user will just try to avoid to do this effort. Obviously we don't want that. If the user bypass the security system ← this is a failure.
  Control : Encryption in smartphone is transparent to the user. We can use our smartphone in the same way with or without (user don't notice it).
  Example of successful attack : Users disabling VPNs, exploited in man-in-the-middle (MITM) attacks (Layer 4).
  Security measure / strategy : Implement Always-On VPNs and user-friendly interfaces

- **Defense in Depth**
  Why : To don't have a single layer of defense → must put many more efforts to attack an infrastructure.
  Control : A multi-layer email system : front-all / backend / firewall / all this component are secured in different way.
  Example of successful attack : DoS attacks (Layer 3).
  Security measure / strategy : Use Content Delivery Networks (CDNs)

- **Fail Safe**
  Why : When a system fails, it should did it in the most secure state.
  Control : (ATM) if power outage : lock the safe == fail secure / The tram : if someone has access to the navigation : stops and open doors == fail safe.
  Example of successful attack : Exploiting a system that reverts to "open" configurations after a failure (Layer 3).
  Security measure / strategy : Configure firewalls to "fail closed" (block everything).

- **KISS (Keep It Simple, Stupid)**
  Why : Easy system is easier to protect.
  Control : Have simple infrastructures reducing the attack surface.
  Example of successful attack : ARP Spoofing (Layer 2) ← poorly managed network configurations.
  Security measure / strategy : Enable Access Control Lists (ACLs).

- **Open Design**
  Why : Security should not rely on secrecy of design ← must be rebust enough even if every know it.
  Control : Shared secret (security by obscurity) / put on the chip.
  Example of successful attack : Exploiting WEP (Wifi Protected Access) (Layer 2).
  Security measure / strategy : Migrate to secure, open standards (e.g., WPA3).

- **Least Common Mecanism**
  Why : Minimize the shared ressources among users ← reduce the risk of interference.
  Control : Security mecanisms that are not are the same level
  Example of successful attack : Exploiting shared servers in side-channel attacks (Layer 4).
  Security measure / strategy : isolate critical process, if one is attacked, the other can be safer.

- **Weakest Link**
  Why : The most vulnerable part of a system will be the first target for an attacker, the security of a system is the security of its weakest point.
  Control : goal for an attacker = admin account / We already know what we must protect.
  Example of successful attack : SSH brute-force attacks (Layer 7 / Maybe the 8 too).
  Security measure / strategy : Double factor authentication + strong password policies.

- **Leveraging Existing Components**
  Why : Reusing tested and secure components reduces risks and speeds up deployment compared to building everything from 0.
  Control : Use known librairies / frameworks…
  Example of successful attack : custom encryption imlpementations (Layer 5).
  Security measure / strategy : → don't use your own crypto.

- **Audit and Accountability**
  Why : Important to track actions to analyse them when incidents occurs.
  Control : Enable logging mecanisms : SIEMs (Security Information and Event Management) ← monitor and analyse actions of users.

Example of successful attack : Undetected intrusion via a compromised VPN (Layer 4).
Security measure / strategy : Strict firewall rules.

- **Defense Against Known Threats**
  Why : Already have a secure system against known vulnerabilities is a saving of time.
  Control : Some patches are here to bring solutions to existing vulnerabilities. Keep applications up to date.
  Example of successful attack : DNS cache poisoning (Layer 3).
  Security measure / strategy : DNSSec ← secure DNS queries.

- **Redundancy and Resilience**
  Why : Systems must withstand and recover from failures (or attacks).
  Control : backups, failover systems.
  Example of successful attack : Network outages causes by BGP hijacking / Route spoofing (Layer 3).
  Security measure / strategy : Firewall with anti-spoof policy.

- **Continuous Improvement**
  Why : Threat landascape evolve → the security must evolve too.
  Control : Perform periodic security assessments and incorporate lessons learned ← into policies and procedures.
  Example of successful attack : Log4j ← exploitation of unpatched vulnerabilities (Layer 7).
  Security measure / strategy : Update standards (new security policies).

- **User Education and Awareness**
  Why : Users = weakest link in security, prevention can avoid many phishing results for example.
  Control : Do security training and awarness campaigns.
  Example of successful attack : Spearphishing <- steal VPN credentials (Layer 7).
  Security measure / strategy : train users with new threats.

- **Risk Management**
  Why : Finite ressources ← prioritize mitigating the highest risks to align with their risk tolerance.
  Control : Risk assessments and frameworks (NIST / ISO) to evaluate and address threats.
  Example of successful attack : Exploiting and overlooked service (Layer 7).
  Security measure / strategy : Monitor critical resources.

- **Security Standards and compliance**
  Why : stick to the standard = security measures meet industry best practices and regulatory requirements.
  Control : Align policies with standards like ISO 27 001 ← ensure compliance.
  Example of successful attack : Non-compliance with PCI DSS exposing sensitive data (Layer 7).
  Security measure / strategy : Do audit regularly ← ensure compliance.