wpriders INTERNAL TEAM BRIEFING

ISO 27001: Strengthening Our Information Security



ISO 27001 CERTIFICATION – WHAT IT MEANS FOR US

- We’re officially pursuing ISO/IEC 27001:2022 certification.
- It’s the international standard for an Information Security Management System (ISMS).
- **Objective**: Protect confidentiality, integrity, and availability of company and client data.
- ISO 27001 aligns us with best practices in data protection and risk management.

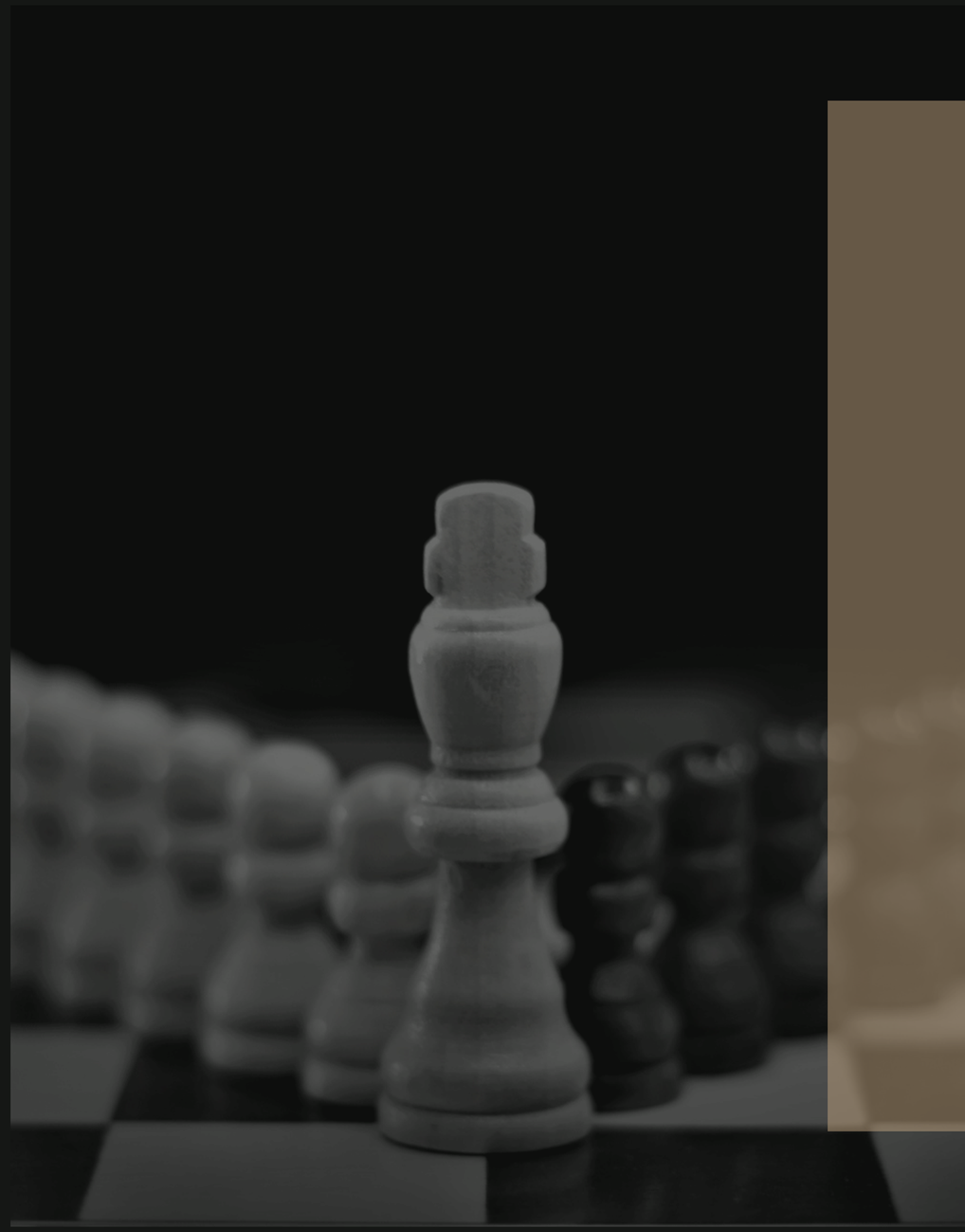
WHY ISO 27001 MATTERS

📈 **Business Credibility**: Clients expect data protection; this certifies we meet global standards.

📄 **Legal & Regulatory Compliance**: Helps meet GDPR and other industry-specific regulations.

🔐 **Risk Reduction**: Identifies and addresses data risks before they cause damage.

🤝 **Client Trust**: Demonstrates to clients, partners, and investors that we take security seriously.



WHAT'S AN ISMS?

A structured system of policies, procedures, responsibilities, and controls.

Ensures secure data handling, risk assessment, access control, and incident response.

Continuously monitored and improved.

Requires leadership commitment, employee awareness, and internal audits.

KEY ISO 27001 REQUIREMENTS WE MUST MEET

🧠 Understand external/internal business context (why security matters to us).

🔍 Identify all stakeholders and their security expectations.

🎯 Define the scope: What systems, teams, and data are covered.

📄 Establish a clear Information Security Policy.

⚙️ Implement risk assessment and risk treatment processes.

🔁 Commit to continual improvement and audits.







INTERNAL MEASURES ALREADY IMPLEMENTED AND IN PROGRESS

✅ Updated password policy in LastPass

✅ Mandatory Google Authenticator for 2FA

✅ No USB storage or data transfer allowed on company devices

✅ Work laptops: No personal use or software installation without written approval

✅ VPN access for external collaborators (in progress)

✅ Strict internal rules against sharing company info externally



PASSWORD POLICY – NO MORE CLEAR TEXT

- All credentials must be saved in LastPass.
- Entries must include:
- Descriptive title (e.g., Stripe - Main Account)
- Correct login URL
- Passwords must not be stored in Google Docs, Notion, email, etc.
- LastPass access logs are audited regularly.

TWO-FACTOR AUTHENTICATION (2FA) WITH GOOGLE AUTHENTICATOR

- Mandatory for all LastPass users.
- ❌ Other 2FA tools are no longer accepted (e.g., Authy, SMS).
- 🎯 Why Google Authenticator:
  - Offline secure codes
  - Uniform adoption = easier management
- Must be set up immediately to avoid lockouts or disciplinary action.

LAPTOP USAGE POLICY (EMPLOYEES & FULL-TIME CONTRACTORS)



NO USB devices for data transfer allowed



No storing:

- Personal files (photos, music, etc.)
- Client files from other jobs
- Side project data



No software installs unless approved via Asana task



Violations = Disciplinary action (see rulebook on Garage)

Contractors – Additional Security Protocols

- 🔐 Will receive VPN credentials for secure remote access
- Until VPN is in place:
- Only access data through approved environments
- Do not download or store any client/company files locally
- No remote desktop tools (e.g., AnyDesk, TeamViewer) unless approved

DATA SHARING & COMMUNICATION RESTRICTIONS

- 🚫 Do NOT share client data, internal docs, or company info:
- On public forums
- With former employees
- On personal devices
- ❗ Even “harmless” sharing (like screenshots in DMs or Slack outside company) can lead to serious violations
- ✅ When in doubt, ask the ISO Officer or IT Manager



WHAT ARE THE RISKS IF WE DON’T COMPLY?

- ❗External ISO audit = real consequences:
- Failure = certification denied
- Repeated violations = loss of clients, legal trouble
- 🚫 Internal actions:
  - Warnings, access revocations, contract terminations
  - Let’s avoid penalties by working as one secure team 💪







HOW WE MONITOR COMPLIANCE

- 🔍 Regular internal audits and self-checks
- ✅ VPN and access logs monitored weekly
- 🛠️ Security incidents documented in ISO log
- 📤 Reports must be submitted if:
  - Data is lost
  - Unauthorized access is suspected
  - Malware is installed or detected



YOUR ACTION ITEMS

- ✓ Make sure your LastPass entries follow the policy
- ✓ Use Google Authenticator for all 2FA logins
- ✓ Review and follow laptop usage policy
- ✓ Ask before installing any software
- ✓ Don’t share internal info externally
- ✓ Report any issues immediately



QUESTIONS? CONCERNS?

Reach out to:

- Your manager
- Our IT Security Officer
- Or check the documentation in Garage