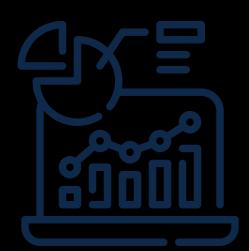
♥ Compliance Checklist:

Ensuring Actsoft® Regulatory Adherence

This checklist helps ensure your mobile workforce is protected and compliant, minimizing risks and safeguarding sensitive data.







Understand Data Regulations

- Stay up-to-date on local, national, and industry regulations.
- Regularly review compliance requirements specific to your industry to avoid costly penalties.



⊘ Implement Data Encryption

- Encrypt all data transmitted between mobile devices and your central system.
- Protect sensitive information from unauthorized access and potential breaches.



Secure Mobile Devices

 Mandate two-factor authentication and regularly updated antivirus software on all work devices.



Train Your Mobile Workforce

- Ensure employees understand their role in safeguarding data and following compliance protocols.
 - Provide regular training on data protection practices.



Back-Up Data Regularly

- Automate frequent data backups to secure, compliant cloud storage.
- Ensure backups are encrypted and easily restorable in case of data loss or breach.

Establish a Mobile Device Policy

- Implement a company-wide policy for mobile device use.
- Outline security protocols and procedures for reporting lost or compromised devices.

Conduct Regular Compliance Audits

- Stay Updated on Emerging Threats
- Schedule audits to assess adherence to regulatory standards.
- Schedule audits to assess adherence to regulatory standards.



 Continuously monitor new security threats, software vulnerabilities, and regulatory changes.



Partner with Trusted Solutions

 Choose mobile workforce management solutions with built-in compliance features like encryption, user authentication, and automated reporting.



Actsoft offers digital solutions for your workforce to help you gain a competitive edge and foster long-term growth and ROI for your business.

https://www.actsoft.com/request-a-demo/