

Written Information Security Program (WISP)

Dealership WISP template, covering what the FTC Safeguards Rule asks for in 16 CFR 314.3 and 314.4.

Dealership and rooftops covered

Qualified Individual

Senior person overseeing the Qualified Individual

Version and effective date

Next review due

How to use it. This is the cover document of your program. Fill in each section with your Qualified Individual, controller, F&I director and IT. Where a section points to a separate part (risk assessment, inventory, vendor register, incident response plan), file that part behind this document and list it in the parts index at the end. Sign it, date it and keep every version.

1 Purpose, scope and objectives 314.3(a), (b)

What the program protects and where. Include every rooftop, department and related entity that shares systems. Objectives: keep customer information secure and confidential, protect it from anticipated threats, and prevent access that could cause substantial harm or inconvenience to a customer.

Dealership, rooftops and entities covered

Customer information in scope

Program objectives

Effective date and version

2 Qualified Individual and oversight 314.4(a)

One person oversees, implements and enforces the program. If that person works for a service provider or affiliate, the dealership keeps responsibility for compliance, names a senior person to direct and oversee them, and requires the provider to maintain its own program that protects the dealership.

Qualified Individual (name, employer)

Senior person who oversees them

Provider program on file (if outside)

Date appointed

3 Risk assessment 314.4(b)

The program is based on a written risk assessment. Point to it here and copy over the highest-scoring risks.

Date of current assessment

Where it is filed

Highest-scoring risks

Next assessment due

4 Access controls and MFA 314.4(c)(1), (c)(5)

How access is granted, limited to what each person needs, reviewed and removed. Multi-factor authentication for anyone accessing any information system, unless the Qualified Individual approves an equivalent or stronger control in writing.

How access is granted and removed

MFA coverage

Written MFA exceptions and approval

Access review owner and schedule

Physical access to paper files

5 Data, devices and systems 314.4(c)(2)

Inventory of the data, personnel, devices, systems and facilities the business runs on, ranked by importance. Keep the full list as its own part.

System or place	Customer information it holds	Importance (1 to 3)	Owner
DMS			
CRM and BDC tools			
F&I menu and e-contracting			
Credit bureau and lender portals			
Email and Microsoft 365			
File server and scanned deal jackets			
Laptops and phones			
Paper deal jackets and old deal files			
Backups			
Other			

6 Encryption 314.4(c)(3)

Customer information is encrypted at rest and in transit over external networks. Where infeasible, list the compensating control and the Qualified Individual approval.

System	At rest	In transit	Exception and compensating control	Approved by, date

7 Applications, changes and monitoring 314.4(c)(4), (c)(7), (c)(8)

How you check the security of purchased and in-house applications, how changes to systems are approved and recorded, and how the activity of authorized users is logged and reviewed.

How purchased and in-house apps are checked

Change approval process

Activity logging and who reviews it

8 Retention and disposal 314.4(c)(6)

Securely dispose of customer information no later than two years after last use for that customer, unless needed for business, required by law, or targeted disposal is not reasonably feasible. Review the retention policy periodically.

Records kept and the reason

Disposal method for paper

Disposal method for drives and devices

Last retention policy review

9 Testing and monitoring 314.4(d)

Regularly test or monitor key controls. Without effective continuous monitoring: annual penetration testing based on the risk assessment, and vulnerability assessments at least every six months and after material changes.

Continuous monitoring in place (what)

Last penetration test, next due

Last vulnerability assessment, next due

Where results go

10 People and training 314.4(e)

Security awareness training updated to reflect the risk assessment; qualified security personnel (staff or provider) who receive security updates and stay current on threats.

Training topics and schedule

Completion tracking

Security staff or provider

How they stay current

11 Service providers 314.4(f)

Select providers able to safeguard customer information, require safeguards by contract, and assess them periodically based on the risk they present. Keep the vendor register as its own part.

Vendor	What it holds or can reach	Security terms in contract?	Last review
DMS provider			
CRM			
Credit bureau connection			
E-contracting or F&I platform			
IT and security provider			
Payroll			
Website and chat			
Other			

12 Incident response and FTC notice 314.4(h), (j)

Point to the written incident response plan (goals, internal processes, roles and authority, communications, remediation, documentation, review after an event). If a notification event involves the information of at least 500 consumers, notify the FTC as soon as possible and no later than 30 days after discovery, on the form on [ftc.gov](https://www.ftc.gov).

Where the plan is filed	
Incident lead	
Owner of the FTC notice	
Last tabletop exercise	

13 Annual report and program review 314.4(g), (i)

At least annually the Qualified Individual reports in writing to the board, or to a senior officer if there is no board: overall status and compliance, and material matters such as risk decisions, service providers, test results, security events and recommended changes. Adjust the program after testing, material changes and new risk assessments.

Who receives the report	
Last report date	
Changes made this year	
Next review date	

Parts index

The separate parts filed behind this cover document. 314.3(a) allows one or more readily accessible parts.

heliontechnologies.com/wisp-template-for-dealerships/

Part	Rule	Where it is kept	Owner	Last updated
Risk assessment	314.4(b)			
Inventory of data, devices and systems	314.4(c)(2)			
Access and MFA standard	314.4(c)(1), (c)(5)			
Vendor register	314.4(f)			
Testing reports	314.4(d)			
Training records	314.4(e)			
Incident response plan	314.4(h)			
Annual report to the board or owner	314.4(i)			
Other policies				

Qualified Individual, signature and date

Owner or general manager, signature and date

Want a second set of eyes on your WISP?

Bring it to a complimentary IT and cybersecurity assessment.

heliontechnologies.com/it-assessment/

Based on 16 CFR Part 314, Standards for Safeguarding Customer Information, as of October 2026. Dealerships with customer information on fewer than 5,000 consumers are exempt from 314.4(b)(1), (d)(2), (h) and (i) under 314.6, but the program itself must still be written. This template is a planning aid, not legal advice. © 2026 Helion Technologies.