

Incident Response Plan

Dealership incident response plan template, covering the seven areas in 16 CFR 314.4(h).

Dealership and rooftops covered

Plan owner (Qualified Individual)

Version date

Next review date

How to use it. Fill in every blank with real names and mobile numbers, give each role a backup, then print two copies and keep them off the network. Run a tabletop drill with everyone named here at least once a year, and update the plan after every drill and every security event.

1 Goals and scope 314.4(h)(1)

What this plan protects and what sets it off. Customer information in the DMS, CRM, email, F&I and paper deal jackets is in scope. A security event is any unauthorized access to, or disruption or misuse of, those systems or that information.

Stores and systems covered

What counts as an incident here

Goals of this plan

2 Response team and decision authority 314.4(h)(3)

Who leads, who backs them up, and who may make the expensive calls. Every role gets a second name.

Role	Name	Mobile	Backup
Incident lead			
Can take systems offline			
Can approve outside spending (limit \$____)			
Speaks for the dealership			
Rooftop contact			
Rooftop contact			

3 Contact sheet 314.4(h)(4)

Print this page. A contact list stored on the network is gone when the network is.

Who	Company or name	24-hour phone	Account or policy no.
IT and security provider			
DMS provider support			
Cyber insurer claims line			
Breach counsel			
Bank fraud line			
FBI field office or IC3 (ic3.gov)			
Floor plan lender			
OEM contact			

4 The first hour 314.4(h)(2)

Report it to the incident lead. Unplug the affected machine from the network but leave it powered on. Do not wipe, reinstall or pay anything until the security team says so.

How staff report an incident _____

Who disconnects what _____

Where the first notes go _____

5 Investigate and size it 314.4(h)(2), 314.4(j)(2)

Which stores, systems and customer records are involved, and was information copied out or only locked? Discovery is the first day any employee other than the attacker knew.

Systems and stores affected _____

Records involved (type and count) _____

Date and time discovered _____

Taken, locked or both _____

6 Communications 314.4(h)(4)

Who says what to staff, customers, lenders, your OEM, vendors and the press. One person speaks to reporters.

Staff script owner _____

Customer letter owner _____

Lender, OEM and vendor notices _____

Media contact _____

7 Notification deadlines 314.4(h)(4), 314.4(j)

Complete the notification sheet at the start of every incident, with counsel. Note why each notice does or does not apply.

FTC notice owner _____

States where affected customers live _____

Insurer notice deadline (from the policy) _____

8 Recover and fix the weakness 314.4(h)(5)

Confirm backups are clean before restoring, reset passwords and MFA, and close the way the attacker got in.

Who checks the backups

Who resets passwords and MFA

Who confirms the fix

9 Keep the record 314.4(h)(6)

Keep a log from the first report to the all-clear: times, decisions, who was called, what was disconnected and what it cost. Use the incident log page.

Log keeper

Where the log is stored

10 Review and update 314.4(h)(7)

After every security event, review what worked and what did not, update this plan and date the new version. Drill at least once a year and after a new store, a DMS conversion or a change in a named role.

Review owner

Last drill date

Next review date

Notification sheet

Section 7. Complete at the start of every incident, with counsel.

heliontechnologies.com/incident-response-plan-template/

Who	Rule or source	Deadline	Applies? Why	Owner	Date sent
Federal Trade Commission	16 CFR 314.4(j)	30 days from discovery, if unencrypted data on 500+ consumers was acquired			
State attorneys general and residents	Each state's breach law	Varies by state			
Cyber insurer	Policy notice clause	Per policy			
Law enforcement (FBI, IC3)	Voluntary	No fixed federal deadline			
Lenders, OEM, DMS and other vendors	Each agreement	Per contract			
SEC (publicly traded groups only)	Form 8-K, Item 1.05	Generally 4 business days after deciding it is material			

Incident log

Section 9. Start at the first report and keep it going until the all-clear.

Date and time	What happened or was decided	Who

Want a second set of eyes on your plan?

Bring it to a complimentary IT and cybersecurity assessment.

heliontechnologies.com/it-assessment/

Areas from 16 CFR 314.4(h), Standards for Safeguarding Customer Information, as of October 2026. Dealerships with customer information on fewer than 5,000 consumers are exempt from the written plan under 314.6; the FTC notice in 314.4(j) applies at any size. This template is a planning aid, not legal advice. © 2026 Helion Technologies.