Vermont 13 V.S.A. Chapter 87 — Computer Crimes

Current Law (as of 2025 session) vs. Draft Amendment

Prepared March 25, 2026

Current Law	Proposed Amendments	Analysis / Notes
§ 4101. Definitions		
9 defined terms: Access, Computer, Computer network, Computer program, Computer software, Computer system, Data, Property, Services. No definitions for cloud services, malicious code, protected computers, or personal identifying information.	**12 defined terms:** Access, Cloud service, Computer, Computer network, Computer program, Computer system, Data, Malicious code, Personal identifying information, Property, Protected computer, Services. Adds 4 new modern definitions. Retains Computer program, Property, and Services.	**Key fix:** The original draft dropped Computer program, Property, and Services. These are still referenced in §§ 4103–4105 and must be retained. **New terms** bring Vermont in line with federal CFAA concepts and other states' modern statutes.
"Access": instruct, communicate with, store data in, enter data in, retrieve data from, or otherwise make use of any resources of a computer system or computer network.	**"Access":** instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resource of a computer, computer system, cloud service, or computer network.	Adds "cloud service" to the definition. Drops "enter data in" as redundant with "store data in." Minor, noncontroversial modernization.
"Computer": electronic device performing logical, arithmetic, and memory functions by manipulation of electronic, photonic, or magnetic impulses, including all input, output, processing, storage, software, or communications facilities.	**"Computer":** electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, storage, or communication functions, including mobile devices, embedded systems, or Internet-connected devices.	Substantially broadened to cover IoT, mobile phones, embedded controllers, and devices not contemplated in 1999. This is the most significant definitional expansion.
§ 4102. Unauthorized Access		
Mens rea: "knowingly and intentionally and without lawful authority." **Conduct:** accesses any computer, computer system, computer network, computer software, computer program, or data. **Penalty:** 6 months / $500, or both.	**Mens rea:** "knowingly and intentionally and without lawful authority." (Preserved) **Conduct:** accesses or causes to be accessed any computer, computer system, cloud service, computer network, computer program, or data. **Penalty:** 1 year / $1,000, or both.	**Critical fix:** The original draft (a) dropped "intentionally," (b) changed "without lawful authority" to "without authorization," and (c) provided NO penalty at all. All three are corrected. Penalty modestly increased to reflect modern realities. "Causes to be accessed" is new and covers using automated tools or botnets.

Side-by-Side Comparison: Current 13 V.S.A. Chapter 87 vs. Draft Amendment

Current Law	Proposed Amendments	Analysis / Notes
§ 4103. Access to Computer for Fraudulent Purposes		
(a) Three prohibited purposes: (1) scheme to defraud; (2) obtaining money/property/services by false pretenses; (3) in connection with fraud, damaging/destroying/altering/deleting/copying/removing programs or data. **Penalty tiers:** (1) ≤$500 first offense: 1 yr / $500; (2) ≤$500 subsequent: 2 yrs / $1,000; (3) >$500: 10 yrs / $10,000.	(a) Four prohibited purposes: original three preserved, plus new (4): obtaining or disclosing personal identifying information or confidential data. **Penalty tiers:** Identical to current law.	**Critical fix:** The original draft completely replaced § 4103 with the aggravated crime section, eliminating all fraud provisions. The revision preserves § 4103 and adds a fourth prohibited purpose to address data theft/disclosure. Preserving the tiered penalty structure avoids creating a "cliff" where minor fraud has no penalty and only the aggravated tier applies.
§ 4104. Alteration, Damage, or Interference		
(a) Prohibits intentionally and without lawful authority altering, damaging, or interfering with operation of any computer, computer system, network, software, program, or data. **Penalty tiers:** (1) ≤$500 first: 1 yr / $5,000; (2) ≤$500 subsequent: 2 yrs / $10,000; (3) >$500: 10 yrs / $25,000.	(a) Same prohibition, expanded to include cloud services and to enumerate modern attack methods: (1) introduction of malicious code; (2) denial-of-service attacks; (3) encryption or disabling of data/systems. **Penalty tiers:** Identical to current law.	**Critical fix:** The original draft silently repealed § 4104 by not mentioning it at all. That would have left malware, ransomware, and DDoS attacks without a stand-alone offense provision. The revision preserves § 4104 and modernizes it. Enumerating modern attack vectors (malicious code, DDoS, encryption) provides clarity for prosecutors and courts without changing the penalty structure.
§ 4105. Theft or Destruction		
(a)(1) Prohibits intentionally depriving owner of possession, taking, transferring, copying, concealing, retaining, or destroying computer systems, networks, software, programs, or data. (a)(2) Safe harbor for copying commercially available software valued ≤$500 not for resale. **Penalty tiers:** Same as § 4104.	Preserved in full with no substantive changes. Safe harbor retained. **Penalty tiers:** Identical to current law.	**Fix:** The original draft silently repealed this section. The revision preserves it intact. The safe harbor for low-value software copying is particularly important to retain—removing it without discussion would be a policy change that could face opposition.
§ 4105a. Aggravated Computer Crime (NEW)		
No equivalent in current law. Current chapter has no aggravated tier or enhanced penalties for large-scale or critical-infrastructure cyberattacks.	(a) Applies when any § 4102–4105 violation also: (1) causes >$5,000 damage; (2) involves a protected computer; (3) exposes PII of 50+ individuals; (4) disrupts critical infrastructure; or (5) involves ransomware.	**Key structural fix:** Placed at § 4105a (not § 4103) so it does not overwrite the fraud provisions. References all four substantive offenses as predicates.

Current Law	Proposed Amendments	Analysis / Notes
	Penalty: 15 years / $50,000, or both. (c) Non-exclusion clause: prosecution does not preclude other charges.	The aggravated tier is the principal new content of the amendment. The 15-year maximum (increased from the original draft's 10 years) positions Vermont competitively with federal CFAA penalties. Policy choices to flag: the 50-person threshold, the $5,000 floor, and whether "critical infrastructure" needs its own definition.
§ 4106. Civil Liability		
A person damaged by a violation may bring a civil action for damages, costs, fees (including reasonable attorney's fees), and other appropriate relief.	Preserved in full. Adds discretionary treble damages for willful violations.	**Fix:** The original draft silently dropped § 4106 entirely, which would have eliminated the private right of action for victims. This is a critical remedy that incentivizes private enforcement. Treble damages for willful violations is a new addition. This is a policy choice; it strengthens deterrence but may face pushback.
§ 4107. Venue		
Violation is committed in Vermont if Vermont is the state from or to which any use of a computer or computer network was made, by wires, electromagnetic waves, microwaves, or any other means.	Preserved. Updated to add "computer system, cloud service" to the list of covered instrumentalities.	**Fix:** The original draft silently dropped § 4107. Without a venue provision, prosecuting out-of-state actors who target Vermont systems would be significantly more difficult. Adding cloud service to the venue provision is important because cloud-based attacks may not involve a "computer network" in the traditional sense.
Summary: Issues in Original Draft Corrected by Revision		
Original draft issues:	**How each is resolved:**	**Why it matters:**
1. No penalty in base § 4102	Penalty restored: 1 yr / $1,000	Without a penalty, the offense is unenforceable.
2. Mens rea lowered to "knowingly" only	"Knowingly and intentionally" restored	Dropping "intentionally" risks vagueness challenges and overcriminalization.

Side-by-Side Comparison: Current 13 V.S.A. Chapter 87 vs. Draft Amendment

Current Law	Proposed Amendments	Analysis / Notes
3. § 4103 (fraud) overwritten by aggravated tier	§ 4103 preserved; aggravated tier at § 4105a	Eliminating the tiered fraud offense leaves a gap between misdemeanor access and the aggravated felony.
4. §§ 4104–4105 silently repealed	Both sections preserved and modernized	Losing stand-alone alteration/damage and theft offenses removes prosecutorial tools for mid-level cybercrime.
5. § 4106 (civil liability) dropped	Preserved with treble damages addition	Victims need a private right of action for cybercrime damages.
6. § 4107 (venue) dropped	Preserved with cloud service update	Essential for jurisdiction over remote and cloud-based attacks.
7. Definitions for Computer program, Property, Services dropped	All three restored in revised § 4101	These terms are used in surviving sections; removing definitions creates ambiguity.