WAC 308-29-085 Remote work requirements. A licensee may allow qualified employees to perform collection activities from virtual offices if the following requirements are met:

(1) **Employee list.** A licensee must keep a record of employees who are permitted to perform collection activities from a virtual office. The list must be kept current, and must include the employee's name, telephone number and email address, and the virtual office location address.

(2) **Equipment list.** A licensee must maintain a current record of licensee equipment supplied to an employee for use in their virtual office.

(3) **Employee remote work agreement.** A licensee must provide the employee a written agreement or checklist signed by the employee that indicates the employee has reviewed and agrees to the following requirements:

(a) While working remotely, the employee must agree to maintain confidentiality of consumer data, must maintain all collection agency data electronically and may not print hard copies or otherwise reproduce copies of collection agency data.

(b) The employee must read and agree to comply with the licensee's IT security policy and any updates.

(c) Employee must agree to maintain the safety and security of licensee's equipment at all times as more particularly described by the licensee.

(d) An employee must review a description of the specific type of collection work the employee or class of employee is allowed to perform while working from their virtual office.

(e) The employee must agree not to disclose or convey to the consumer that the employee is working from a virtual office or that the virtual office is a place of business.

(f) An employee must be advised that the employee's collection agency activities are subject to review and calls to and from the virtual office will be monitored and recorded.

(4) **Virtual office requirements.** An individual employee's virtual office is an extension of the licensee's business office and must meet the following requirements:

(a) It must have full connectivity with the licensee's business office systems including computer networks and phone system and must provide the licensee the same level of oversight and monitoring capacity as if the employee were performing their activities in the business office.

(b) It must have the capability to record calls made to and from the virtual office and to monitor virtual office calls in real time.

(c) It must be located within the United States and, within one hundred miles of the licensee's business office.

(d) It must be in a private location where the employee can maintain consumer confidentiality during the performance of their collection activities.

(e) It must meet all security requirements of this section and contain the equipment necessary to conduct the licensee's work safely and efficiently.

(f) Each employee shall be connected to the business office via a virtual office that requires unique credentialing for access by each employee.

(g) No more than one employee may work from a virtual office from the same physical location, except that cohabitating employees may each maintain a virtual office from their shared residence.

(h) Employees may not print or store physical records in the employee's virtual office.

(5) **Employee requirements.** The licensee is responsible for ensuring that an employee working from a virtual office meets all of the following requirements:

(a) To become eligible to work from a virtual office, the employee must have completed a training program at the licensee's business office, which covers topics including compliance, privacy, confidentiality, monitoring and security, and other issues that apply particularly to working remotely from a virtual office.

(b) In addition, an employee must complete a minimum of forty-five days of direct oversight and mentoring in the licensee's business office prior to working from a virtual office. This requirement may be waived by the board under emergency circumstances that the board has determined makes it impossible to perform.

(c) Once an employee begins to work from a virtual office, they must be subject to the same levels of communication, management, oversight and monitoring via telecommunications and computer monitoring as they would if working in the business office.

(d) While working remotely the employee must comply with all applicable laws and regulations as outlined in chapters 19.16 and 18.235 RCW and chapter 308-29 WAC.

(6) **IT security requirements.** Licensees are responsible for developing and following a written IT security policy for virtual offices that outlines the security protocols in place safeguarding the company and consumer data. Consumer data in the form of an electronic record must have the appropriate protections against unauthorized or accidental disclosure, access, use, modification, duplication, or destruction.

The IT security policy shall include the following additional requirements:

(a) Virtual office access to the collection agency's secure system must be through the use of a virtual private network "VPN" or other system that requires usernames and passwords, frequent password changes, authorization, multifactor authentication, data encryption, and/or account lockout implementation.

(b) The immediate installation or implementation of any system updates or repairs in order to keep information and devices secure.

(c) The provision of safe and secure storage with expandable capacity for all electronic data including consumer and licensee data.

(d) Virtual offices must contain computers and/or other electronic devices that have secure computer configurations and reasonable security measures such as updated antivirus software and firewalls.

(e) Access to licensee's systems must occur on company-issued computers and electronic devices whose use is restricted to authorized employees while working at their virtual office, and an employee's use of devices must be limited to employment related activities on behalf of licensee.

(f) Consumer data is accessed securely through the use of encryption or other secure transmission sources.

(g) An action plan has been developed and communicated with relevant employees on how to handle a data breach arising from remote access devices in accordance with applicable laws, which shall include any required disclosures of such breach.

(h) A disaster recovery plan has been developed and communicated with relevant employees on how to respond to emergencies (e.g., fire,

natural disaster, etc.) that have the potential to impact the use and storage of licensee's data.

(i) The secure and timely disposal of licensee's data as required by applicable laws and contractual requirements.

(j) An annual internal or external risk assessment is performed on the collection agency's protection of licensee's data from reasonably foreseeable internal or external risks. Based on the results of the annual risk assessment, the collection agency shall make adjustments to its data security policy if warranted.

(k) The licensee can stop the virtual office's connectivity with the network and remotely disable or wipe company issued computers and electronic devices that contain or have access to licensee's information and data when an employee no longer has an employment relationship with the company.

(7) **Call recording and monitoring.** Licensees must consistently record and monitor calls in which employees are performing collection activities. Call recordings must be maintained for a minimum of four years and call monitoring must be regularly performed, a portion of which must be in real time. Recording and monitoring calls from virtual offices must meet industry standards for collection agencies and ensure that virtual office calls comply with chapter 19.16 RCW and more particularly with RCW 19.16.250 (13)(c), (18), and (19) and also chapter 9.73 RCW.

(8) **Nondisclosure.** Neither the employee nor the licensee shall represent to debtors or any other party that the employee is working independently from licensee in a virtual office. Such acts include, but are not limited to:

(a) Advertising in any form, including business cards and social media, an unlicensed address or personal telephone or facsimile number associated to an unlicensed location.

(b) Meeting consumers at, or having consumers come to the employee's virtual office.

(c) Holding out in any manner, directly or indirectly, by the employee or licensee, an address that would suggest or convey to a consumer that the virtual office is a licensed collection agency location or "branch office," including receiving licensee's mail, or storing books or records at the virtual office.

It shall not be considered a violation of this section if, in response to an inquiry about the remote worker's location, a remote worker responds that the worker is working remotely or working from a virtual office, or words to that effect.

(9) **Data breach.** Should a licensee or virtual office experience a data breach as defined under chapter 19.255 RCW, the licensee must comply with the requirements of chapter 19.255 RCW.

(10) **Evaluation.** The board will review and evaluate the adequacy of this section at least annually and will make amendments, as the board deems necessary.

[Statutory Authority: RCW 19.16.351. WSR 21-03-046, § 308-29-085, filed 1/14/21, effective 2/14/21.]