AMENDATORY SECTION (Amending WSR 01-11-132, filed 5/22/01, effective 6/22/01)

WAC 308-29-010 Definitions. (1) Words and terms used in these rules have the same meaning as each has under chapter 19.16 RCW unless otherwise clearly provided in these rules, or the context in which they are used in these rules clearly indicates that they be given some other meaning.

(2) "Branch office" is any location physically separated from the principal place of business of a licensee where the licensee conducts any activity meeting the criteria of a collection agency or out-of-state collection agency as defined in RCW 19.16.100.

(3)"Business Office" is the licensed principal place of business or certified branch office from which the licensee conducts the business of a collection agency.

((~~(3)~~))(4) "Employee" is a person employed by a licensee and shall not be deemed a "collection agency" or a "branch office" as defined in RCW 19.16.100 (5)(a) so need not have an additional license or certificate to perform collection activities on behalf of the

licensee whether working from a business office or from the employee's virtual office.

(5) "Repossession services" conducted by any person shall not be deemed a collection agency as defined in RCW 19.16.100, unless such person is repossessing or is attempting to repossess property for a third party and is authorized to accept cash or any other thing of value from the debtor in lieu of actual repossession.

(6) "Managing employee" is an individual who has the general power to exercise judgment and discretion in acting on behalf of the licensee on an overall or partial basis and who does not act in an inferior capacity under close supervision or direction of a superior authority (as distinguished from a non-managing employee who is told what to do and has no discretion about what he or she can and cannot do and who is responsible to an immediate superior).

[Statutory Authority: [RCW 19.16.410]. WSR 01-11-132, § 308-29-010, filed 5/22/01, effective 6/22/01; Order PL-123, § 308-29-010, filed 5/17/72.]

(7) "Remote work" occurs when an employee performs collection activity for a licensee from the employee's "virtual office" as defined herein and more particularly described in WAC <<>>.

(7) "Virtual Office" is a virtual extension of the licensee's business office, which is fully connected via electronic means and telecommunications to the business office and its employees and from which an individual employee may perform the same work and be similarly monitored as if physically located at the business office and as more particularly described in WAC <<>>.

NEW SECTION

WAC 308-29-085 Remote work requirements. Licensees that allow eligible employees to work from a virtual office must ensure that the following requirements are met:

(1) **Employee List.** A record of which employees are eligible and have been permitted to work remotely from a "virtual office" must be maintained and kept current.

(2) **Remote Work Agreement.** Each eligible employee and licensee agree to and sign a Remote Work Agreement, which will contain the following:

- Employee's name, remote contact information including virtual office location address, telephone number and email address;

- Agreement to maintain confidentiality of consumer data while working remotely.
- List of Security specifications and requirements that the employee and licensee must maintain at all times;
- List of Equipment supplied and to be used by the employee to enable them to work remotely and meet the requirements of chapter 19.16 RCW and this WAC;
- A description of the specific type of collection work the employee is allowed to perform while working remotely.

(3) **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 licensee the same level of oversight and monitoring capacity as if the employee were performing their activities in the business office.

b. It must be located within the United States and within 100 miles of the licensee's business office.

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

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

e. Each employee shall be connected to the business office via their own virtual office system, which shall not be used by any other employee or for any other purpose.

f. No more than one employee may work from a virtual office from the same physical location, except that co-habituating employees may each maintain a virtual office from their shared residence.

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

a. Prior to being eligible to work remotely, the employee must have completed a training program at the licensee's business office, which covers topics including compliance, confidentiality, monitoring and security; and must have worked

for the licensee for a minimum of thirty (30) days prior to working remotely.

b. 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.

c. 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.

(5) **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 customer data, information and electronic and physical records, to protect them against unauthorized or accidental access, use, modification, duplication, destruction or disclosure. Physical records must be stored and maintained at the business location and may not be stored at the remote work location. Non-managing employees may not print or store physical records in the employee's virtual office.

The licensee's written IT security policy shall be on file at the licensee's business prior to allowing employees to work remotely.

(6) **IT Security Policy.** The licensees shall develop and comply with an IT security policy that includes the following requirements:

a. Virtual office access to the collection agency's secure system from a company-issued computer or other electronic device through the use of a virtual private network "VPN" or other system that requires passwords, frequent password changes, identification authentication authorization, multifactor authentication, data encryption, and/or account lockout implementation.

b. Any updates or other requirements in order to keep information and devices secure.

c. The safe and secure storage of electronic data;

d. Computers and 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 that only the employee is authorized to use and 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; and

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 Monitoring.** Licensees must record and monitor all calls initiated or received by their employees while employees are working remotely and must maintain copies of these recordings and make them available for inspection upon request. All calls must comply with RCW 19.16.250 (13)(c), (18), and (19).

(8) **Non-Disclosure.** Neither the employee nor the licensee shall conduct any activity that would indicate or tend to indicate the employee is working from 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.

(9) The provisions of this section, WAC 308-29-085 and WAC 308-29-010(6) "virtual office" shall expire at the conclusion of the Governor's declared state of emergency in response to new cases of COVID-19, directing state agencies to use all resources necessary to prepare for and respond to the outbreak.

[]