Remote Desktop Protocol (RDP)

Purpose and Scope

In response to the need for agency staff to work from home or alternate locations due to the COVID-19 pandemic, this document outlines the security and use of RDP for teleworking or telecommuting.

In General

Remote access has always been a critical part of the State's computing environment. It allows us to extend the continuity of our services outside the confines of our physical offices. The use of RDP is highly secure and just as safe as working in your physical office. **But you are part of assuring that security**.

> *Remember: just like you must practice safe and secure computing practices at work, you must do the same at home. That doesn't change!*

We want to enable you to work effectively at anytime and anywhere to serve our citizens; therefore, we ask for your help to ensure we keep our citizen information and sensitive data secure.

RDP

Delaware's Remote (RDP) Access is first secured with a leading IT remote access solution. This solution creates a secure connection through the internet to the state computing environment. This secure connection acts as a dedicated tunnel, allowing a remote worker to travel into our state network and to a dedicated device/computer. When you RDP you are working on a device that resides in the office. The State of Delaware information remains safe and security on that device, even when you are accessing it remotely. We monitor the network and that device for attacks just like we do every day when you are in the office.

Secure 2-Factor Authentication

To access this dedicated tunnel there are multiple factors that must be validated. The first factor is a very secret piece of information: your very own username and password. The second factor is usually a special software code generated by a smartphone application or a one-time code sent to your phone as a text. State employees that previously had remote desktop permission will continue to use this method. In response to the increased and immediate demand for teleworkers due to COVID-19, we established a different secondary factor. The first factor remains the same, the second factor for COVID teleworkers utilizes a dedicated computer at work. The combination of these two things makes it almost impossible for the bad actors to create or access your private tunnel without you.

Telecommuting Workspace

Employees should establish and maintain a dedicated workspace that is quiet, safe and secure.

Remote Desktop Protocol (RDP)

Employees must comply with all State of Delaware and Agency security procedures and ensure security measures are in place to protect equipment and data from physical and virus damage, theft, loss, or access by unauthorized individuals. This includes protection from other family members or people who are present during working hours or who access the employee's computer.

Safeguarding Customer Information

As a State of Delaware employee, you are responsible for safeguarding the confidentiality and integrity of data in State computer files regardless of the source of those data or the medium on which they are stored. We have a responsibility to our citizens to comply with all applicable privacy laws and regulations. It is a serious breach of policies, and in some cases of the law, to use citizen information for anything other than business purposes. As we work together through this unprecedented COVID-19 pandemic situation, we must take every precaution available to minimize external parties ability to overhear customer conversations or view/access data transmissions.

Acceptable Use Policy

The full version of the State's Acceptable Use Policy can be viewed at:
https://dti.delaware.gov/security/delaware-acceptable-use-policy-self-test/