National Association of State Retirement Administrators

Responses to survey regarding work from home policies and practices

Twenty-eight systems in 24 different states responded to this survey; a listing of responding systems is at the end of these results. This survey was conducted in August 2020.

1. *Does your retirement system have a written policy governing employees working remotely?*

   Yes: 20

   No: 8

2. *If your system has a policy, was the policy developed as a result of the pandemic, or was this policy in place prior to the pandemic?*

   Policy was developed prior to the pandemic: 13

   Policy was developed in response to the pandemic: 6

   We do not have a policy for working remotely: 8

   Other responses given

   - The policy was in place prior to the pandemic, but it was updated during the pandemic.

3. *Please identify which groups of employees, if any, apply to the following condition:*

   Eligible to work remotely:

   - All (7)
   - All except essential employees/those whose duties will not allow (8)
   - As a response to the pandemic, we are allowing employees who are able to complete job responsibilities remotely with health or childcare issues to work remotely at the discretion of their division director
   - Decisions as to who may work remotely are made on a case by case basis. Most of our administrative, accounting and customer service personnel are capable of remote work.
   - Been employed more than six months, have at least "effective" performance, be able to work independently, work in a role that lends itself to remote work.
   - Investments, Finance, Legal, Executive, IT.
   - Managerial discretion.
   - Technically, no employees are "eligible" to work remotely. Almost all employees, except for some staff in operations, are working under a temporary telework arrangement.
   - Majority of staff. Remote connectivity dictates ability to work remotely.

   Ineligible to work remotely:

   - Call Center staff
   - IT Personnel & Member Service Representatives (Reception/Phones)

Contact: Keith Brainard keith@nasra.org or Alex Brown alex@nasra.org

- Front desk
- Mailroom staff
- Those who cannot perform essential services remotely
- It's up to the manager of the department but typically managers and supervisors would only telecommute on an ad hoc basis.
- Workers whose job requires resources only found in the building (Facilities Services, Mail Center, Print shop, etc.).
- Essential staff needed to maintain remote operations

Required to work remotely:

- During the pandemic, those who can perform their work remotely
- Field representatives
- Employees who are under quarantine who are able to complete their job responsibilities remotely
- Staff deemed to be "at risk"
- All except essential staff

4. *For employees who are eligible or required to work remotely, what requirements, if any, are in place to be present physically in the retirement system offices (one day a week, every other day, etc.) Are any employees forbidden from entering the retirement system offices? If so, which employees?*

Selected responses

- Those working remotely must be in the office two (variable) days a week. This is subject to change based on conditions. No employees are forbidden from entering the system's offices.
- Pre-COVID: It was up to the respective Director to determine what job titles and how many days per week someone could work remotely within in their division. The maximum people could work remotely was 2 days per week. Overall, Internal Audit, Communications and IS were the main departments that had staff working remotely. No one was forbidden from coming to the system offices, however our Field Representatives have always worked 100% remotely.

  During COVID: All employees are working varying days in the office and/or at home. As of today, we have about 50% of our staff in the office at any given time. Once the pandemic is over, we will evaluate a more standardized telecommuting policy.
- Remote Staff must check with their manager to enter the building. Managers coordinate the number of staff and time in the building to ensure social distancing, i.e. not too many at one time.
- No one is forbidden to enter the offices; all managers were required to maximize telework consistent with getting the work done. In practice, on any given day, we are about 66% teleworking and 34% in the office. Things have evolved; in the member benefits section we were platooning the operation week to week with 1/2 in the office, 1/2 at home and then switch the following week. We've since found it better to work this more on a day in / day out system, so most benefit specialists have about two days in the office in a given week and about 3 days telework.
- One-third (3 managers) work onsite regularly. Remote staff are not allowed in the building and access credentials are terminated. If a staff person must come to the building, they undergo a wellness screening in advance of arriving.

- No employees are forbidden to enter the system offices, even at this point in time (unless they have to quarantine because of illness or traveling to a ""hot spot"" state). All non-essential employees (see above) at this point in time are allowed to work in the building up to 100% of the time (0-100%).

  Outside of the pandemic environment, employees who want to work remotely are allowed to do so only one day per week.

- Remote workers are fully remote. They must get permission from their senior manager to enter the building. This is to maintain the safety of the small essential workforce that is needed to process incoming payments and documents so that the rest of the employees can do their work remotely.

5. *For employees who work remotely, what office supplies and equipment does the system provide?*

   Selected responses

   - Computer, monitor, keyboard, mouse, telephone, headset, etc.
   - We provide system-issued laptops, monitors (if needed), laptop bags, etc. For staff working 100% remote (Field Reps) we provide system-issued cell phones and vehicles, since they travel around the state as well. Although Internal Audit does not work 100% remote, they also have cell phones and vehicles available for use. We are currently working on getting the Call Center the ability to work 100% remote, so they will also receive headphones.
   - Prior to pandemic: teleworking optional. staff provided their own equipment

     During pandemic: teleworking is required. staff without proper equipment will be provided proper equipment

     Post-pandemic - has not yet been determined
   - The system provides a laptop and VPN access to employees working remotely. Employees are allowed to use whatever supplies from their offices that are necessary to complete their job duties. Upon request, a Mifi (portable Internet accessible device) can be provided.
   - All equipment including adjustable height work station if ergonomically required. Moved to a cloud-based phone system in July to accommodate remote workers.
   - We have also supplied printers, envelopes and postage for a few administrative staff to help with sending correspondence that is not system generated such as letters from the Director's office.
   - Employees may request to take their office chair home as well.
   - We have a few employees who are using personal devices for WFH; however we are transitioning as quickly as we can to system-owned devices only. Most employees have a system-owned laptop or encrypted desktop and dual monitors at home. We do not allow them to use this for personal/family use. They are not allowed to connect a home device to system-owned equipment.
   - Currently, we are providing whatever IT equipment is needed for associates to work remotely because of the pandemic, which includes taking home desktop machines if necessary.

Outside of the pandemic, employees can use their system-issued laptops for remote work, but cannot remove desktop machines. We also would not provide any additional equipment for them to work remotely (e.g., provide a laptop if they have a desktop).

- We provide a laptop and mouse. Work cellphone if desired. Many employees use their own cellphone under a "Bring your own device" policy with secured applications. Employees were allowed to take monitors and keyboards home. A few employees took their office chair home.

6. *Please describe any cyber-security systems that are in place for employees working remotely.*

Selected responses

- We work in a VDI environment for full access to system network and non VDI for modified access to perform work and access system materials/work. All fully supported thru security system.
- A new Cybersecurity curriculum was created to emphasize work from home security best practices, while continuing to adhere to existing data protection standards. Various delivery methods were employed to address adoption of topics; from interactive videos to daily emails covering remote work security tips.
- Our system's network infrastructure was scaled to provide the needed technology performance to handle increased demands on computer, email, and communication conferencing programs.
- Required operating system requirements and approved anti-virus software. Employees are also trained on cyber security monthly.
- We use multi-factor authentication, VPN/RDS and require WFH users to use only a secured internet service (pwd protected, updated). We have minimum os and virus scanner requirements for personally-owned devices being used for system work. We had a third party review of the WFH setup and make recommendations that we are implementing to increase security. We are considering supplying routers to each WFH employee to ensure they are uniformly updated and secured.
- To access VPN, we utilize Cisco AnyConnect. Employees must first log into Cisco AnyConnect using a third party authentication code, then they are allowed to access their office desktop through VPN.
- Multifactor authentication. Monitoring of connections. Log tracking and evaluation through two vendor partners.
- Our system, through SOM Cybersecurity and Infrastructure Protection department, has robust cyber-security infrastructure, training and procedures prior to the pandemic. The system distributes routine reminders and trainings to maintain employee knowledge of security and abuse protocols specific to the system such phishing, data transfer breaches, and identification fraud.
- RDS app. We use KnowBe4 for security awareness training and have stepped up the training during the pandemic.
- Our remote access (telework) solution resides within the system Firewalls (FW). Secure connectivity is managed by the Cisco Virtual Private Network (VPN) requiring multi-factor authentication (MFA) per user. Within the FW, the system is using the security platform called Fire Eye Endpoint Security that continuously monitors (CM) and tracks anomalies providing reports. These reports are then disseminated by the OA Archer Security through the Commonwealth Enterprise Information Security Office (EISO).

Our system is currently undergoing product review and evaluations for a system-specific Data Loss Prevention (DLP) solution. With DLP, the system will have the capability of Real-time reporting and management of incidents as well as, alert users when Personally Identifiable Information (PII) and other security sensitive information is being transferred or stored.

Both the Fire Eye Endpoint Security Platform and the perspective DLP solution protect remote users and monitor information security incidents and alerts within the SER/OA FW's.

- Everyone has a JVPN account to log into the state's network and Cisco Jabber is used for answering phones through our laptops and for the chat function internal to our system.
- McAfee login for laptops and FortiClient two-factor authentication to access the network.
- SSL VPN was in place prior to the pandemic for normal remote users and for disaster recovery processing. We have had to activate our Disaster Recovery licensing to accommodate the amount of remote workers.

  Factors in use now that we have had well before the pandemic include two-factor authentication for any remote access; intrusion prevention systems; data loss prevention systems; malware detection systems; and all E-Mail processing inbound/outbound.

  Partially due to the increased remote workforce, we have added further redundancy to our firewall systems and have purchased additional SSL VPN licenses. Otherwise, all controls and their associated expenses (from an IT Security perspective) were in place prior to the pandemic."

- We enabled Duo authentication software which sends a code to your registered device (usually a cellphone) whenever you log in with user id and password. The code must also be entered. We do not allow employees to print at home. If anyone tries to download a file to a thumb drive, there is instant notification to security. A file downloaded to a desktop is part of the system's network. Employees using their own cellphones access email through Boxer, which allows us to remotely wipe the phone in the event it is lost or there is an employee termination.

7. *Do you expect your system's policy and practice regarding employees working remotely to change after the current pandemic, and if so, in what ways?*

   Selected responses

   - Yes. The experience teleworking has taught us that it is possible for certain divisions to be more productive using telework than in the building. We will be open to each division finding the right balance between work from home and in the office to maximize productivity. In rough terms, I suspect that we will see about 50% of work done remotely ranging from full-time work from home employees to full-time in the office (and every possible combination in between).
   - I expect our WFH policy to be the same post-pandemic. We anticipate that we will have approximately 50% of our staff continue to WFH for at least 2-3 days per week going forward.
   - Yes, the standard telework policy will likely be reworked to make it a little less complicated and not require so much documentation. The policy will likely envision most employees doing some telework, either due to weather, childcare, or delivery issues (the

new refrigerator is coming today) as well as a likely requirement to demonstrate this about once a month just for business robustness and continuity of operations.

- We are reviewing future working arrangements. Currently, we are considering have approximately 25% of staff work remotely on any given day when staff return to the office.
- Yes. I expect that we will return to a policy of no remote work. There could be limited exceptions on a case by case basis.
- We are likely to have people working from home more days than they used to (more than half of the week for many). All the possible decisions resulting from this are still being discussed, including: office equipment (user provides, agency provides), internet capability (user provides, agency provides), office space (sharing and/or downsizing of physical office and how to effectuate)
- Yes, broader use of working remotely by supervisory and managerial staff, evolved flexible work schedules and enhanced virtual learning; strategies that support an engage hybrid (on-site/off-site) workforce and workplace culture
- Remote work is only eligible for those impacted or potentially impacted by COVID-19. There was no remote working in the history of the organization prior to the pandemic. The retirement system will not be implementing a long-term remote work policy option.
- Our current policy was used in very limited scenarios - generally as accommodations for health reasons. We quickly created WFH ""guidelines"" that we expect each WFH employee to follow and created a website for tips as well, but we have not yet created a policy because we want to set policy based on post-pandemic circumstances.

  Post-pandemic changes:
  1. Require employees to enter the building periodically
  2. Require speed minimums on home internets
  3. Require that WFH employees acquire childcare/adult care services as they would if they were coming in to the office
  4. Require turn on video from home for meetings"
- The system conducted an employee survey to measure teleworking engagement for employees (management access, computer equipment, isolation, etc). Based on employee feedback, the system anticipates offering some type of teleworking option/s for some positions following the pandemic. At this time, teleworking models would follow existing SOM policies and guidelines that existed prior to the pandemic. Existing teleworking policies are written and maintained by the SOM Office of State Employer.
- Still being discussed. Consideration is being analyzed for flexibility of member service delivery by using virtual methods and extend hours of operation.
- Yes, although we had remote workers before, there will be a larger adoption of remote working now that it has been shown to be possible with continued productivity.

8. *Please share any other observations or pertinent information regarding your system's experience with remote work policies.*

   Selected responses

   - Ours is a rural state with less than ideal connectivity options and then presents logistical challenges for some staff. The balance of suggesting they upgrade and requiring it is a policy discussion we have yet to tackle.
   - Business metrics such as retirement application processing and telephone service level have overall not been negatively impacted due to teleworking. Data also shows a decrease in staff absenteeism.

- Telecommuting has been ideal for the winter weather in our state. Based on the forecast, we will ask our Information Center to work from home. They appreciate the flexibility from a personal level and we insure that service to our members is uninterrupted. Overall, our employees have been very happy with the program and our service levels remain high.
- We have seen how much paper we rely on and are working to change manual procedures to electronic.
- The pandemic has pushed us to remote faster than we would have otherwise implemented. We also see benefits to changing our business continuity plans. However, we are seeking ways to maintain communication and culture when most of our staff are working from home.
- Additionally, our childcare and school concerns have impacted our remote work policy. Our "Return to Office" Committee continues to meet regularly to discuss, and if necessary, to recommend changes to the policy as necessary to Executive Leadership.
- One of the challenges has been replacing written signatures with electronic ones on internal administrative workflow. Our member communications were mostly electronic already, but internally we still required signatures on employee hires, budget transfers, contracts, etc. These have mostly been accommodated via emailing Adobe pdfs but it is clunky.

Responding Systems:

- Retirement Systems of Alabama
- Arizona State Retirement System
- Arkansas State Highway Employees' Retirement System
- California State Teachers' Retirement System
- Hawaii Employees' Retirement System
- Illinois Municipal Retirement Fund
- Iowa Municipal Police & Fire Retirement System
- Kentucky Retirement Systems
- Louisiana State Employees' Retirement System
- Maine Public Employees' Retirement System
- Michigan Office of Retirement Services
- Municipal Employees' Retirement System of Michigan
- Minnesota Public Employees' Retirement Association
- Public Employees' Retirement System of Mississippi
- Missouri DoT & Highway Patrol Employees' Retirement System
- Missouri Public School & Educational Employee Retirement System
- New Hampshire Retirement System
- Ohio Public Employees' Retirement System
- Ohio School Employees Retirement System
- Oregon Public Employees' Retirement System
- Pennsylvania Public School Employees' Retirement System
- Pennsylvania State Employees' Retirement System
- Employees' Retirement System of Rhode Island
- South Carolina Public Employee Benefit Authority
- Tennessee Consolidated Retirement System
- Employees Retirement System of Texas
- Teacher Retirement System of Texas
- Washington State Department of Retirement Systems
- Wyoming Retirement System