Reset Form

CONFIGURATION OF PERSONAL DEVICE TO STATE NETWORK

State Form 55610 (R4/ 9-24)
INDIANA DEPARTMENT OF HEALTH

Purpose: *For agency workforce members that do not have state-issued equipment but would like to utilize their private mobile devices to receive their state-issued email, calendar, contacts, and applications. IOT provides alternative access for individuals who have obtained approval from both their director and assistant commissioner to synchronize their state credentials with their personal devices. IOT, in collaboration with IDOH, reserves the right to enforce all conditions for all devices connected to the state network as outlined in the Information Resource User Agreement (IRUA).*

Directions: *Use blue or black ink to complete steps 1, 2, and 3. Next, return this form to IDOH Security Manager to complete step 4. Once steps 1-4 has been completed, your appointment will be scheduled to configure your personal device to the state network.*

1. *Print the required information of the individual who will be receiving the device below.*

End-User Information	
Name:	
E-mail Address:	
Contact Number:	
Program Area:	
Supervisor / Manager:	
Personal Cellular Number:	
Personal Cellular Provider:	
Personal Device Make and Model:	
Employment Status	
Are you a state-employee? ☐ Yes ☐ No	If no, who is your vendor?
User Agreement	
By initialing below, I acknowledge that I have read each statement carefully. I also agree that IOT reserves the right to electronically monitor and access data, contacts and applications.	
□ I understand this is considered an Information Resource as explained in the Information Resources Use of Agreement (IRUA) agreement.	
□ All mobile devices require a passcode, which cannot be shared, and changed at least once every six (6) months.	
□ After five (5) minutes of inactivity, devices should be programmed to lock with users being prompted to re-enter their passcode.	
□ Users must keep all firmware updated as prompted by the Telecommunications Manager or IOT.	
□ If your device is lost or stolen, a notification should be submitted to the Information Security Officer and Telecommunications Manager in writing, immediately.	
□ I understand IOT provides remote management services to install and remove data, contacts, and applications. IOT is not responsible for any lost data, contacts, or applications. IOT does not support non-state-issued devices for advanced technical support.	

2. *Obtain the signature of your program area's director.*

Director Approval	
By signing below, I hereby grant permission to the aforementioned staff member to synchronize their personal device to the network to conduct state business. I am aware it is my responsibility to notify the Office of Technology and Compliance of any changes in employment with this individual to terminate the use of their accounts.	
Director Signature	Date *(mm/dd/yy)*

3. *Obtain approval of your program area's assistant commissioner.*

Assistant Commissioner Approval	
By signing below, I agree to allow the requesting user to access their state credentials on their personal device.	
Director Signature	Date *(mm/dd/yy)*

STOP **Do not complete anything else below this line.** STOP

GO **Return this form IDOH Security Manager in the Office of Technology and Compliance.** GO

4. *Obtain approval of the IDOH Security Manager or designee.*

Security Manager Approval			
Reviewed On *(mm/dd/yy)*	Reviewed By	□ Approved	□ Rejected
Comments:			

5. *Once your appointment has been scheduled with Administrative Services, and your device has been configured, you will sign in acceptance of this agreement.*

Signature of Agreement	
Signature of Staff	Date *(mm/dd/yy)*

For Internal Use Only – Office of Technology and Compliance – Communications Manager	
ISSUED BY:	Date *(mm/dd/yy)*