|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Agency Name | Indiana Department of Revenue | | Name your program, idea, or project: | Indiana Department of Revenue Security and Privacy Awareness Training Program | | What is the problem that you wanted to solve? | The Indiana Department of Revenue (DOR) needed a single training program to effectively communicate security guidance that is agency-specific and also meets all compliance requirements. This training needed to be high-quality, accurate, and effectively delivered to 700 team members located in 13 locations. It also had to offer engaging and educational learning of important issues, principles, and practices.  Before developing this new Security and Privacy Awareness training that solved our problem, multiple DOR personnel spent significant time developing, updating, completing and managing two different training programs to meet the IRS’s security awareness, role-based, and disclosure awareness training requirements. The old program and delivery processes were cumbersome, inconsistent, and did not achieve the desired learning goals. In conjunction with the desire to dramatically improve the program’s content and effectiveness, DOR sought to reduce that program management workload by combining and integrating all content into one training program.  One of the two previous programs used a commercial computer-based training (CBT) product that delivered generic, non-agency specific information. It did not effectively communicate the IRS, state, and agency policies to which our DOR teammates are required to adhere. DOR needed a program that incorporates relevant and custom information from multiple internal policies and delivers the resulting guidance in a clear and unified way to all learners.  Both training programs previously in use were lacking in the way they engaged and effectively educated the learner. One program enabled trainees to complete it with minimal engagement. The other sounded like a narrated policy document. The new DOR Security and Privacy Awareness program dramatically improves real learning and the likelihood of the internalization, commitment, and vigilance with which DOR employees transfer what they learn to the job. | | Who was involved in addressing the problem? | A cross-functional DOR Security and Privacy Awareness Training team was developed consisting of team members from the DOR Compliance and Ethics, Inspector General, Legal, Training, and Security Teams. The team developed a cohesive vision of the program including learning objectives, engagement level, content, and the desired end results. | | How did they go about finding a solution? | The project team initiated the DOR Security and Privacy Awareness Training development effort by defining goals for the final deliverable. They shifted the approach to focus on practicing security because it was the right thing to do, and not just because it is something DOR teammates are legally obligated to do. As a result, the project team decided the resulting training program would explain how exercising security demonstrated team members’ adherence to DOR’s core values of fun, leadership, integrity, respect, teamwork, service, and continuous improvement.   Members of the DOR Compliance and Ethics, Inspector General, Legal, Training, and Security Teams then proceeded to develop training scripts. The entire project team subsequently worked collaboratively over many months to review, edit, and enhance those scripts to ensure they covered all the material DOR teammates had to learn, ensure that the tone was appropriate and that each script was achieving the desired objectives for each module. The project team wanted its training to convince and encourage—not direct and threaten. | | Describe the outcome. What is the new idea, approach, program, or activity? | The project team successfully delivered a single DOR Security and Privacy Awareness training program, comprising 13 e-learning modules.  The program fulfills all IRS, National Institute of Standards and Technology, Defense Information Systems Agency, Indiana State, and agency requirements with which DOR teammates must comply. It delivers the combined guidance unambiguously and educates employees on how they must respond to specific security situations.  The training program explains the practical and policy reasons for exercising security, threats and vulnerabilities most relevant to DOR, bad actor methods and tools for exploiting security, and specific actions and tools that should be taken and implemented to protect DOR data and systems. It also, wherever possible, reinforces why and how such actions align with DOR core values.  Upon finalizing the scripts, the project team filmed multiple familiar DOR teammates presenting each topic while dressed in DOR branded clothing, creating a personalized DOR teammate-to-teammate style of communication of the topic.   The new solution is a highly interactive modular e-learning training program. In design, the modules deviate from the more traditional approach where a learner may passively watch a video and then finish by answering a few quiz questions. Interactivity is, instead, built in throughout the video tutorials, with the video pausing to encourage learner participation, agreement, and reflection before continuing. The interactive pause and continue approach provides for reinforcement of critical points such as a must-know point, or a reminder about how applying the instruction aligns with specific DOR core values. Instead of using standard "Continue" or "Advance" text on interactive buttons, the buttons often use phrases such as "I agree" or "Got it!" The modules also include thought-provoking quizzes, scenario-based activities requiring decisions from learners, fun interactive games, pop-up questions, fun animated summaries, and videos of DOR teammates practicing security.  The modular nature of the program means that employees can incrementally complete the program over multiple short sessions, allowing them to complete the learning at their convenience. Unlike previous years, DOR was able to deploy this training to over 700 teammates and achieve 100% completion in only eight weeks.  Learner feedback acquired via a survey built into the final module is overwhelmingly positive. 90% of DOR teammates praised the training for being enjoyable. DOR’s Chief Financial Officer commended it for making the material engaging, informative, and relevant to the agency’s core values. DOR’s Chief Operating Officer called it “very professional and extremely high-quality.” | | What has changed since this was implemented? How have your operations improved? Include any data, analytics or metrics that would show the value of your program. Don't forget management advantages such as improved morale. | DOR has seen several positive changes since Security and Privacy Awareness Training was delivered.  First, team members performed extremely well in a phishing test immediately following its deployment.  Second, the DOR Security Team is receiving noticeably fewer requests for security guidance. Third, the DOR Security Team is also receiving more reports of suspected security violations.  Lastly, the amount of work to administer this program is markedly less than the quantity required to manage the previous separate training programs.  Most important, the program has achieved 100% participation before required deadlines. It also has received very positive reviews.  We have also successfully implemented this program in the new employee onboarding process so that all new team members start off with a solid foundation of security awareness and skill. | | Is this an in-house project, or did you partner with an outside vendor or service-provider? | 100% in-house | | What comes next — will you be adding to your program, rolling it out more widely, trying additional approaches? | The project team will assess and update the training program annually to ensure it reflects the most current policies and procedures, and real-world threats and vulnerabilities. | | |