

|   |  |                                  |
|---|--|----------------------------------|
| <b>POSITION DESCRIPTION</b>                                 |  | AGENCY/DEPT ID<br>DAS500000      |
| DIVISION OR INSTITUTION<br>Office of Information Technology | UNIT OR OFFICE<br>Office of Security & Privacy | COUNTY OF EMPLOYMENT<br>Franklin |

|  |   |  |   |  |
|--|---|--|---|--|
| POSITION NUMBER<br>20073890<br><br>JOB CODE TITLE<br>Information Technology Consultant 3<br><br>JOB CODE<br>64163<br>ATD 3-2-16 VS | <input type="checkbox"/> Reclassification <input type="checkbox"/> New Position <input checked="" type="checkbox"/> Update  |  | Position Hyperlinked to <input type="checkbox"/><br>Agency Organizational Tree  |  |
|  | USUAL WORKING TITLE OF POSITION<br>Threat & Vulnerability Management Program Manager  |  | POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR<br>SEE TABLE OF ORGANIZATION   |  |
|  | <input checked="" type="checkbox"/> Permanent<br><input type="checkbox"/> Temporary<br><input type="checkbox"/> Intermittent  | <input type="checkbox"/> Classified<br><input checked="" type="checkbox"/> Unclassified<br><input type="checkbox"/> Essential  | Overtime: <input type="checkbox"/> Eligible <input checked="" type="checkbox"/> Exempt<br>If FLSA Exempt, exemption type: | Bargaining Unit 22<br>PR - 17<br>Page 1 of 2 |
|  | NORMAL WORKING HOURS (Explain unusual or rotating shift):<br>FROM: 8:00 am                      TO: 5:00 pm   |  |   |  |
| <b>JOB DESCRIPTION AND WORKER CHARACTERISTICS</b>  |   |  |   |  |
| %  | Job Duties in Order of Importance   | Knowledge, Skills & Abilities  |   |  |
| 45   | Leads the development, implementation and ongoing maintenance of an enterprise vulnerability management program; provides technical advice & direction to administrators & assistant administrators regarding any & all facets of information technology (IT) security standards & best practices: recommends & implements IT security standards & best practices to remediate discovered vulnerabilities; collaborates with other technical resources to develop and implement mitigation strategies for discovered vulnerabilities; develops plans for ongoing vulnerability scanning activities; runs vulnerability scanning tools to discover both application and network vulnerabilities; conducts penetration tests and/or coordinates with external penetration testing partners to verify vulnerabilities are exploitable. | <b>Knowledge of</b> (1) computer science; (2) computer security best practices; (3) policy development; (4) business/IT planning; (5) network security measures, equipment & software; (6) Federal statutes, regulations, policies, & guidelines pertaining to computer security; (7) technical writing techniques; (8) TCP/IP protocols; (9) computer hardware systems; (10) integration of firewalls, intrusion detection/prevention systems, users authentication systems, virtual private networks; (11) computer networking both wired & wireless; (12) disaster recovery planning; (13) security architecture; (14) division & agency policies & procedures*;<br><b>Skill in</b> (15) operation of personal computer & associated hardware/software;<br><b>Ability to</b> (16) create & read flowcharts; (17) read pseudocode; (18) interpret extensive variety of technical material in books, manuals, & network/system diagrams; (19) cooperate with coworkers on projects & group activities; (20) maintain security certification [e.g., Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP); Certified Information Systems Auditor (CISA), Certified Information Privacy Professional (CIPP)].<br><br>*developed after employment |   |  |
| List Position Numbers & Job Titles of Positions Directly Supervised:<br><br>SEE TABLE OF ORGANIZATION                              |   | SIGNATURE OF AGENCY REPRESENTATIVE<br><br><i>David A Brown</i>   | DATE<br><br>3/22/16   |  |

|   |  |                                  |
|---|--|----------------------------------|
| <b>POSITION DESCRIPTION</b>                                 |  | AGENCY/DEPT ID<br>DAS500000      |
| DIVISION OR INSTITUTION<br>Office of Information Technology | UNIT OR OFFICE<br>Office of Security & Privacy | COUNTY OF EMPLOYMENT<br>Franklin |

|   |  |   |   |  |  |
|---|--|---|---|--|--|
| POSITION NUMBER<br>20073890<br><br>JOB CODE TITLE<br>Information Technology Consultant 3<br><br>JOB CODE<br>64163<br>APR 3-2-16 | <input type="checkbox"/> Reclassification <input type="checkbox"/> New Position <input checked="" type="checkbox"/> Update   |   |   | Position Hyperlinked to <input type="checkbox"/><br>Agency Organizational Tree   |  |
|   | USUAL WORKING TITLE OF POSITION<br>Threat & Vulnerability Management Program Manager   |   | POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR<br>SEE TABLE OF ORGANIZATION   |  |  |
|   | <input checked="" type="checkbox"/> Permanent<br><input type="checkbox"/> Temporary<br><input type="checkbox"/> Intermittent | <input type="checkbox"/> Classified<br><input checked="" type="checkbox"/> Unclassified<br><input type="checkbox"/> Essential   | Overtime: <input type="checkbox"/> Eligible <input checked="" type="checkbox"/> Exempt<br>If FLSA Exempt, exemption type: |  | Bargaining Unit 22<br>PR - 17<br>Page 2 of 2 |
|   | NORMAL WORKING HOURS (Explain unusual or rotating shift):<br>FROM: 8:00 am    TO: 5:00 pm                                    |   |   |  |  |
|   | <b>JOB DESCRIPTION AND WORKER CHARACTERISTICS</b>  |   |   |  |  |
|   | %  | Job Duties in Order of Importance   |   | Knowledge, Skills & Abilities  |  |
|   | 35   | Assist DAS & OIT program administrators & staff in identifying security needs; assists in the development and maintenance of a strategy for response to security breaches; reviews agency mission specific policies & procedures; assists in staff training throughout DAS and other state agencies as necessary. |   | <b>Knowledge of 1-14*</b><br><b>Skill in 15</b><br><b>Ability to 16-20</b>   |  |
|   | 10   | Participates as team member of Office of Information Technology (OIT) Security Incident Response Team: provides subject matter expertise for development of enterprise security standards, policies, procedures & assessments.  |   | <b>Knowledge of 1-14*</b> ; (21) basic computer forensic procedures;<br><b>Skill in 15,</b><br><b>Ability to 16-20</b> |  |
|   | 10   | Performs other administrative functions as required: prepares reports & analyses on assigned administrative & support functions; attends &/or conducts meetings; manages special projects;  |   | <b>Knowledge of 1-13</b><br><b>Skill in 15</b><br><b>Ability to 16-19</b>  |  |
|   |  |   | Position is unclassified per 124.11(A)(9) of Ohio Revised Code.   |  | *developed after employment                  |
| List Position Numbers & Job Titles of Positions Directly Supervised:<br>SEE TABLE OF ORGANIZATION                               |  |   | SIGNATURE OF AGENCY REPRESENTATIVE<br><i>David A Brown</i>  |  |  |
|   |  |   | DATE<br>1/26/16   |  |  |

SRD 1/26/16