


| | |
|---|--|
|  <p>Georgia Department of Community Health</p> | <p>Office of Information Technology, Cybersecurity Office</p> |
|---|--|

INFORMATION SECURITY INCIDENT REPORT FORM

*THIS FORM MUST BE COMPLETED WITHIN 24 HOURS OF DETECTING AN CYBERSECURITY INCIDENT AND
FORWARDED TO THE AGENCY CYBERSECURITY OFFICE: dchois@dch.ga.gov*

| | |
|--|-----|
| 1. SECURITY INCIDENT NUMBER: | SR- |
| 2. CAPGEMINI INCIDENT/SERVICE REQUEST NUMBER (if applicable) | |
| 3. INCIDENT TYPE: <ul style="list-style-type: none"> e.g. HIPAA Security Compliance, Physical Security, Access Control, Cyber-Security Attack, Malware, Asset Theft, Policy Violation, Financial, etc. Note: If the Incident Type is "Malware", update the Malware Incident Checklist in Section 8. | |
| 4. INCIDENT DATE: | |
| 5. REPORT DATE: | |
| 6. REPORT PREPARED BY: | |
| 7. INCIDENT REPORTED BY: NAME: PHONE: E-MAIL: DCH DIVISION: DCH WORK UNIT / SECTION: | |
| MALWARE INCIDENT CHECKLIST: | |
| <input type="checkbox"/> Name and Type of Computer Virus or Malware Infection | |
| <input type="checkbox"/> Available system/ virus removal software log info | |
| <input type="checkbox"/> Impact Assessment Single Workstation, System, Application, Network, or Data? | |
| <input type="checkbox"/> Number and Type of Files or Data Infected | |



Office of Information Technology, Cybersecurity Office

8. POST INCIDENT ACTIVITY:

- Note any Policies or Procedures that require updating.
- Document lessons learned and modify the Incident Response Plan accordingly.
- Recommended Action.

NOTES:

ADDITIONAL INFORMATION: