# Policy Revision Request

Requestor Name Det. W. Pursley Emp # 3778

This revision applies to Existing Policy 08-15-24

If new, recommended section

This revision is necessary to comply with Best Practices

Whom does this revision affect? Department

This revision has an unbudgeted financial impact of $ 0

**Brief reason for the revision:**

Previous versions of policy were more clear regarding the appropriate course of action for submitting physical items containing digital evidence, specifically that they should, in general, be submitted to APD Evidence. The language making that clear was unintentionally removed a few years ago during an update, and this will restore and improve that language.

**Document the changes or additions to the policy below. Please include the specific policy number. ~~Red strikethroughs~~ are used for deletions and blue underlined for text insertions. Please email completed forms to APDPolicy@austintexas.gov. Use this email for any related questions or issues for policy.**

## 618 Property and Evidence Collection Procedures

### 618.4 PHYSICAL EVIDENCE COLLECTION

Employees will assess a crime scene before seizing any item of physical evidence. Only items of physical evidence that relate to allegations of criminal conduct or the identity of a suspect will be seized. Employees will ensure that items identified as evidence are not tampered with in any way prior to being photographed and collected.

*(a) Unchanged from current version*
*(b) Unchanged from current version*

(c) Seized physical items such as cell phones and computers containing original digital evidence requiring forensic analysis will be submitted to the Digital Forensics Unit along with the appropriate request.

1. Employees submitting seized digital evidence to the Digital Forensics Unit shall follow the Department's general orders related to seized evidence processing and submission.

2. Employees should be familiar with the documents: Best Practices for Seizing Electronic Evidence, as well as Searching and Seizing Computers and Obtaining Electronic Evidence, available on the DFU SharePoint site.

3. Evidence seized containing digital evidence will typically be submitted through established evidence recovery guidelines to the Evidence Section. The most common exceptions that exist are:
   (a) Items in need of an Immediate/Call-Out type response by the DFU
   (b) Certain mobile devices which:
      1. were originally seized powered on and have been maintained in a powered on state since seizure,
      2. are locked, and
      3. do not have a known code

   For devices meeting possible exceptions or a more current/exhaustive list, contact the Digital Forensics Unit.

4. Employees shall submit an ATLAS Forensics Analysis Request to the Digital Forensics Unit no later than 30 days after submitting the seized digital evidence.

5. Employees shall not attempt to access seized digital evidence, unless exigent circumstances exist or the employee accesses the evidence at the direction of the Digital Forensics Unit.

~~618.6.6 SUBMITTING SEIZED DIGITAL EVIDENCE~~
~~Employees shall submit all seized digital evidence to the Digital Forensics Unit for analysis.~~

~~(a) Employees submitting seized digital evidence to the Digital Forensics Unit shall follow the Department's general orders related to seized evidence processing and submission.~~

~~(b) Employees shall submit an ATLAS Forensics Analysis Request to the Digital Forensics Unit no later than 30 days after submitting the seized digital evidence.~~

~~(c)~~(a) ~~Employees shall not attempt to access seized digital evidence, unless exigent circumstances exist or the employee accesses the evidence at the direction of a Digital Forensics Unit detective.~~