

HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

----------

PHÒNG CHỐNG & ĐIỀU TRA TỘI PHẠM MÁY TÍNH

**Đề tài: dịch Chapter 1 , 2 , 3 - Global Guidelines For Digital Forensics Laboratories**

Khoa: Công nghệ thông tin

Chuyên ngành: An toàn thông tin

***Giảng viên hướng dẫn:***

# **Thầy: Lại Minh Tuấn**

***Nhóm sinh viên thực hiện:***

**Nguyễn Quang Huy**

**Lưu Hùng Lợi**

**Ngô Thanh Nhã**

**Hà Nội- 2019**

**MỤC LỤC**

[I. GIỚI THIỆU 3](#_Toc26410839)

[1. Mục đích tài liệu 3](#_Toc26410840)

[2. Đối tượng dự định 3](#_Toc26410841)

[3. Áp dụng tài liệu 3](#_Toc26410842)

[II. GIỚI THIỆU VỀ ĐIỀU TRA SỐ 4](#_Toc26410843)

[1. Điều tra số 4](#_Toc26410844)

[2. Hiểu bằng chứng điện tử 5](#_Toc26410845)

[3. Nguyên tắc bằng chứng điện tử 5](#_Toc26410846)

[III. QUẢN LÝ PHÒNG LAB ĐIỀU TRA SỐ 6](#_Toc26410847)

[1. Thực hiện kế hoạch 6](#_Toc26410848)

[2. Cơ sở 8](#_Toc26410849)

[2.1 Vị trí 8](#_Toc26410850)

[2.2 Bảo mật vật lý 9](#_Toc26410851)

[2.3 Kích thước và bố cục 11](#_Toc26410852)

[2.4 Cơ sở 14](#_Toc26410854)

[2.5 Khách 15](#_Toc26410855)

[3. Nhân viên 17](#_Toc26410856)

[3.1 Tuyển dụng 17](#_Toc26410857)

[3.2 Giải phóng mặt bằng an ninh 18](#_Toc26410858)

[3.3 Mô tả công việc 18](#_Toc26410859)

[3.4 Phát triển nhân viên 20](#_Toc26410862)

[3.5 Kèm cặp 22](#_Toc26410863)

[3.6 Sức khỏe và an toàn 22](#_Toc26410864)

[4. Thiết bị 23](#_Toc26410865)

[4.1 Phần mềm 24](#_Toc26410866)

[4.2 Phần cứng 25](#_Toc26410867)

[4.3 Dụng cụ và phụ kiện 25](#_Toc26410868)

1. **GIỚI THIỆU**
2. ***Mục đích tài liệu***

Hướng dẫn INTERPOL cho phòng Lab điều tra số phác thảo các quy trình thành lập và quản lý phòng Lab điều tra số (DFL) và cung cấp các hướng dẫn kỹ thuật để quản lý và xử lý bằng chứng điện tử.

Các nguyên tắc này phải được xem như một tài liệu mẫu có thể được các quốc gia sử dụng khi xem xét phát triển khả năng điều tra số của họ. Lời khuyên đưa ra được dự định sẽ được sử dụng ở cả cấp chiến lược và chiến thuật, phù hợp với luật pháp, thực tiễn quốc gia, và thủ tục.

***2. Đối tượng dự định***

Tài liệu này được các nước thành viên INTERPOL sử dụng. Mục tiêu của những nguyên tắc là đảm bảo rằng bằng chứng điện tử do DFL tạo ra có thể được chấp nhận trong thành viên các quốc gia Tòa án pháp luật cũng như trong các hệ thống tư pháp hình sự quốc tế.

Nguyên tắc tập trung chủ yếu vào hai nhóm riêng biệt: nhóm đầu tiên là các chiến lược gia điều tra số và các nhà quản lý đưa ra quyết định cho DFL; nhóm thứ hai bao gồm các nhân viên kỹ thuật xử lý bằng chứng điện tử hàng ngày.

Ngoài ra, các công tố viên, thẩm phán và luật sư cũng sẽ được hưởng lợi từ tài liệu này trong sự hiểu biết quy trình điều tra số, có thể rất quan trọng đối với các trường hợp của họ.

1. ***Áp dụng tài liệu***

Nguyên tắc không nhằm áp đặt các giới hạn đối với các DFL phải tuân theo yêu cầu của khung pháp lý quốc gia của họ. Lời khuyên được đưa ra trong các nguyên tắc này không nhằm mâu thuẫn với bất kỳ luật pháp quốc gia nào ở bất kỳ quốc gia thành viên nào.

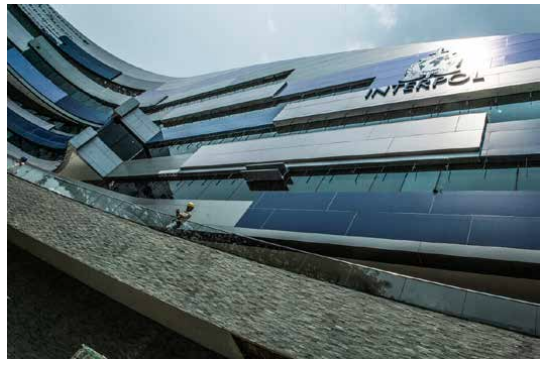
**II. GIỚI THIỆU VỀ ĐIỀU TRA SỐ**

1. ***Điều tra số***

Điều tra số là một nhánh của khoa học pháp y tập trung vào việc xác định, thu nhận, xử lý, phân tích và báo cáo dữ liệu được lưu trữ trên máy tính, thiết bị kỹ thuật số hoặc phương tiện lưu trữ kỹ thuật số khác.

Máy tính, thiết bị kỹ thuật số hoặc hệ thống lưu trữ kỹ thuật số khác chứa dữ liệu quý giá để điều tra được gọi là bằng chứng điện tử. Ví dụ như máy tính xách tay, điện thoại thông minh, máy chủ, đầu ghi hình kỹ thuật số, hệ thống camera quan sát, máy bay không người lái, hệ thống GPS và máy chơi game.

Mục tiêu chính của điều tra số là trích xuất dữ liệu từ bằng chứng điện tử, xử lý dữ liệu thành thông tin hữu ích và trình bày kết luận để truy tố.Tất cả các quá trình liên quan, do đó, nên sử dụng các kỹ thuật pháp y hợp lý để đảm bảo rằng những phát hiện này có thể được chấp nhận tại tòa án.



Bản chất của các trường hợp liên quan đến bằng chứng kỹ thuật số là không biên giới và hành vi phạm tội xảy ra trong tích tắc; do đó, những phát hiện thu được từ bằng chứng điện tử phải làm theo một bộ hướng dẫn tiêu chuẩn để đảm bảo rằng nó không chỉ được chấp nhận tại một quốc gia cụ thể, tòa án của pháp luật, mà còn trong hệ thống tư pháp hình sự quốc tế.. Hướng dẫn INTERPOL về điều tra số cung cấp cơ sở và tài liệu tham khảo cho việc quản lý điều tra số.

1. ***Hiểu bằng chứng điện tử***

Bằng chứng điện tử, không giống như bất kỳ bằng chứng nào khác, chẳng hạn như dư lượng sợi, tóc và súng, là một thách thức để xử lý do thực tế là:

a. Dữ liệu có thể được phân tán ở một số địa điểm, đôi khi trên khắp các quốc gia;

b. Dữ liệu có thể được chuyển qua biên giới tài phán một cách dễ dàng và trong một vấn đề giây;

c. Dữ liệu rất dễ bay hơi - dễ dàng bị thay đổi, ghi đè, bị hỏng hoặc bị phá hủy bởi đột quỵ đơn của một phím;

d. Dữ liệu có thể được sao chép mà không suy giảm;

e. Tuổi thọ của bằng chứng điện tử, không giống như bất kỳ kỷ luật pháp y nào khác, là ngắn trước khi nó vô dụng. Một ví dụ về điều này là một điện thoại thông minh: sau năm năm, nó có thể không thể bật hoặc hoạt động đúng. Do đó, dựa trên những sự thật này, bằng chứng điện tử phải được xử lý và xử lý đúng hạn quan tâm.

***3. Nguyên tắc bằng chứng điện tử***

Khi xử lý bằng chứng điện tử, các nguyên tắc sau phải được tuân thủ:

a. Bằng chứng điện tử phải được thu thập một cách hợp pháp.

b. Nhân viên tham gia phải hoàn thành chương trình đào tạo phù hợp, trước khi xử lý bằng chứng điện tử.



c. Bất kỳ hành động nào được thực hiện trên bằng chứng điện tử không được thay đổi dữ liệu của nó. Nếu cần thiết để truy cập dữ liệu gốc hoặc thay đổi cài đặt hệ thống đề nghị chỉ những nhân viên có năng lực mới có thể làm như vậy,

và nhân viên đó phải có khả năng biện minh cho những hành động đó.

d. Bất kỳ hành động nào yêu cầu dữ liệu gốc được truy cập hoặc thay đổi nên được ghi lại và chứng kiến ​​bởi một đồng tu nếu có thể.

e. Một bản ghi của tất cả các hành động được thực hiện khi xử lý bằng chứng điện tử phải được tạo và bảo quản để chúng có thể được kiểm toán. Một bên thứ ba độc lập sẽ có thể lặp lại những hành động đó và đạt được kết quả tương tự.

**III. QUẢN LÝ PHÒNG LAB ĐIỀU TRA SỐ**

Phần này giải thích quá trình thiết lập DFL - tạo kế hoạch, đạt được yêu cầu tài nguyên và các hoạt động liên quan đến việc duy trì DFL.

***1. Thực hiện kế hoạch***

Nghiên cứu ban đầu phải được thực hiện để thiết lập số liệu thống kê gần đây về việc thu giữ bằng chứng điện tử, các loại tội phạm, địa điểm, chuyên môn của các cảnh sát bắt giữ và liệu có phân tích pháp y kỹ thuật số đã được thực hiện.Thông tin cần cung cấp một hướng dẫn công bằng về sự tăng trưởng của điều tra kỹ thuật số và phục vụ như là một chỉ dẫn về nơi bắt đầu. Thông tin này cũng sẽ giúp cơ quan xác định nhu cầu đầu tư cũng như quy mô của DFL.

Mỗi cơ quan phải tìm cách hiểu các yêu cầu pháp lý hoặc thủ tục trong việc việc thành lập DFL trong hệ thống tư pháp hình sự của đất nước.

Điều này có thể được thực hiện thông qua so sánh với các quốc gia có địa lý tương tự và nhân khẩu học tương tự đã thiết lập DFL, để cung cấp sự hiểu biết vững chắc về các yêu cầu để thiết lập một DFL. Tìm câu trả lời cho các câu hỏi sau đây sẽ giúp người ra quyết định hiểu và nhận ra phạm vi của DFL:



a. Có bao nhiêu cuộc điều tra về các tội phạm được báo cáo đã được tạo điều kiện thuận lợi với việc sử dụng dữ liệu số trong 3 năm qua, 2 năm và 1 năm?

b. Có một sự tăng trưởng rõ ràng và được ghi nhận trong loại điều tra này?

c. Nếu điều tra kỹ thuật số được yêu cầu;

• Ai đã tiến hành phân tích?

• Những thủ tục đã được tuân theo?

• Kết quả là gì?

• Chi phí của các kỳ thi là gì?

• Có phải là không thể thực hiện một số chức năng do thiếu tài nguyên?

d. Có các cơ quan thực thi pháp luật khác ở quốc gia có yêu cầu tương tự mà sự hợp tác có thể được bắt đầu để đẩy nhanh việc chấp nhận đề xuất DFL không?

Thiết lập một DFL đòi hỏi vốn và chi phí hoạt động. Chi phí vốn bao gồm chi phí thiết bị và phần mềm và có được và tân trang lại cơ sở thích hợp.

Đây là những chi phí một lần của người Viking yêu cầu cho cơ sở hạ tầng và thiết bị,trước khi bắt đầu giai đoạn vận hành.

Chi phí hoạt động sẽ bao gồm các chi phí hoạt động như thuê tòa nhà, phí giấy phép phần mềm, lương nhân viên, đào tạo nhân viên, bảo trì thiết bị pháp y và thay thế thiết bị văn phòng.

Một khi nghiên cứu ban đầu này được thực hiện, những người ra quyết định nên có một ý tưởng tốt hơn về vai trò và quy mô của DFL, cũng như số lượng nhân viên cần thiết để cung cấp một nguồn lực hiệu quả cho tất cả các bên liên quan.

***2. Cơ sở***

Khi chọn các tiền đề để xây dựng DFL, một số yếu tố cần được xem xét để đảm bảo thành công của nó. Các phần sau đây sẽ giải thích chi tiết các yếu tố thành công có thể có khi lựa chọn và phát triển DFL.

*2.1* *Vị trí*

Một số yếu tố cần được xem xét khi chọn vị trí của DFL. Một số mối quan tâm cần được giải quyết là:

|  |  |
| --- | --- |
| Cân nhắc chọn vị trí DFL | |
| 1 | Có đủ năng lượng điện để chạy các thiết bị cần thiết không, thiết bị bổ sung có cần bổ sung cho các cơ sở năng lượng được lắp đặt (máy phát điện dự phòng / UPS) không? |
| 2 | Nếu phòng thí nghiệm ở trên tầng trệt, có thang máy để vận chuyển số lượng lớn bằng chứng điện tử không? |
| 3 | Tòa nhà hoặc văn phòng có đủ mạnh để đảm bảo an toàn cho dữ liệu và bảo vệ người dân bên trong không? |
| 4 | Các bức tường, sàn và trần nhà có đủ mạnh để chống lại thiệt hại vật lý hoặc môi trường không?  Có thiệt hại về môi trường không? |
| 5 | Rủi ro từ lũ lụt, hỏa hoạn, thiên tai và bất ổn dân sự là gì? |
| 6 | Sự quan tâm đúng mức có được thực hiện để giảm thiểu rủi ro bị tấn công bởi một tổ chức khủng bố hoặc tội phạm đang tìm cách gây thiệt hại cho các cuộc điều tra? |
| 7 | Tòa nhà có phù hợp để cung cấp việc làm mát cần thiết cho số lượng thiết bị được đặt trong tòa nhà, hoặc các cơ sở làm mát có thể được trang bị thêm không? |

**Bảng 1**. Cân nhắc chọn vị trí DFL



*2.2* *Bảo mật vật lý*

DFL không chỉ cần bảo mật bằng chứng điện tử mà còn đảm bảo an ninh cho nhân viên, phần mềm và phần cứng có giá trị. Danh sách kiểm tra về bảo mật vật lý như sau:

|  |  |
| --- | --- |
| Danh sách kiểm tra về an ninh vật lý | |
| 1 | Hệ thống giám sát  Hệ thống giám sát được sử dụng để giám sát các cơ sở để truy cập trái phép và đột nhập. Các chuyên gia cài đặt nên xem xét vị trí chiến lược tốt nhất cũng như độ phân giải tốt nhất để đảm bảo an ninh tối đa. |
| 2 | Kiểm soát truy cập  Kiểm soát truy cập có thể ở dạng khóa và phím vật lý, bàn phím điện tử, thẻ quẹt và / hoặc sinh trắc học, tùy thuộc vào ngân sách. |
| 3 | Hệ thống kiểm soát cháy  Một DFL phải có hệ thống phát hiện cháy và hệ thống chữa cháy được lắp đặt tại cơ sở. Vật liệu được sử dụng cho hệ thống chữa cháy không được gây thiệt hại cho tang vật, thiết bị hoặc nhân sự. |
| 4 | Cửa sổ, cửa và tường bảo vệ  Khi được yêu cầu, các cửa sổ nên được gia cố bằng các thanh và khóa để tránh đột nhập. Nếu DFL có cửa sổ và tường bằng kính, cần chú ý rằng dữ liệu nhạy cảm sẽ được bảo vệ khỏi tầm nhìn. Cân nhắc sử dụng cửa chống cháy ở vị trí như cầu thang hoặc hành lang để bảo vệ cơ sở khỏi hỏa hoạn. |
| 5 | Có đủ ổ cắm điện, cầu chì, cầu dao và tải hiện tại  Phải lắp đặt đủ ổ cắm, cầu chì và cầu dao trong DFL để đảm bảo vận hành trơn tru và ngăn ngừa quá tải điện dẫn đến nguy cơ hỏa hoạn và gây rủi ro cho sự an toàn của nhân viên. |
| 6 | Sàn chống tĩnh  Sàn chống tĩnh điện giúp giảm khả năng phóng tĩnh điện (ESD) có thể gây hại cho nhân viên, thiết bị và bằng chứng. |
| 7 | Hệ thống gây nhiễu radio  DFL nên cài đặt một hệ thống để chặn tín hiệu mạng, ví dụ như sử dụng lồng Faraday hoặc thiết bị gây nhiễu. Một hệ thống gây nhiễu Radio sẽ chặn bất kỳ tín hiệu mạng nào và ngăn chặn mọi sự xâm nhập vào triển lãm. Với công nghệ không dây hiện tại, khả năng các điện thoại thông minh hoặc máy tính xách tay được bật nguồn có thể tự động kết nối với các mạng không dây hiện có, do đó sửa đổi dữ liệu của họ. Pháp luật quốc gia phải được kiểm tra để xác minh rằng việc sử dụng các hệ thống như vậy được cho phép và chúng không can thiệp vào các hệ thống khác. |
| 8 | Hệ thống làm mát  Thông thường, một DFL có máy tính để thực hiện công việc, tạo ra một lượng nhiệt đáng kể trong phòng thí nghiệm. Quá nóng có thể dẫn đến mất dữ liệu và làm hỏng phần cứng. DFL nên cài đặt một hệ thống làm mát để kiểm soát nhiệt độ phòng, bao gồm phòng lưu trữ bằng chứng và phòng máy chủ. |
| 9 | Sao lưu dữ liệu ngoài trang web  Một lượng lớn dữ liệu được DFL lưu trữ sau khi nó hoạt động đầy đủ và về bản chất nó có thể nhạy cảm. Dữ liệu thường được lưu trữ trong một máy chủ. Cách tốt nhất là dữ liệu được sao lưu vào máy chủ ngoại vi, cách xa DFL. Trong trường hợp thảm họa mà DFL bị ảnh hưởng, bộ nhớ ngoại vi có thể được sử dụng để có quyền truy cập vào dữ liệu quan trọng. Có một bản sao lưu lưu trữ dữ liệu ngoại vi là một phần của kế hoạch khắc phục thảm họa nhằm đảm bảo các hoạt động có thể được thực hiện và chạy trong thời gian tối thiểu. |
| 10 | Lưu trữ dữ liệu lưu trữ / Lưu trữ dữ liệu dài hạn  Sau khi phân tích, dữ liệu nên được lưu trữ sao cho chúng có thể được truy xuất vào một ngày sau đó nhằm mục đích tiếp tục quá trình xử lý hoặc xem xét các bằng chứng hoặc phát hiện mới liên quan đến vụ án. Thời gian lưu trữ phải được điều chỉnh theo yêu cầu pháp lý quốc gia. |

**Bảng 2**. Danh sách kiểm tra về an ninh vật lý

*2.3 Kích thước và bố cục*

Tối thiểu, một DFL phải bao gồm các bảng để bàn để Giám khảo tiến hành phân tích, một bảng lớn để đăng ký bằng chứng, ghi nhãn, chụp ảnh và niêm phong, tủ chống cháy để lưu trữ bằng chứng điện tử và tủ hồ sơ. Thiết lập tối thiểu này là đủ cho một DFL quy mô nhỏ, nơi gửi một lượng nhỏ bằng chứng điện tử.

Tuy nhiên, đối với một cơ quan liên quan đến một số lượng lớn bằng chứng điện tử, thiết lập tối thiểu này có thể không đủ. DFL nên phân tách các loại hoạt động cụ thể để ngăn ngừa lây nhiễm chéo và mất các tang vật.

Ví dụ, phải có một khu vực để nhận bằng chứng. Điều này có thể được thực hiện trong việc tiếp nhận, trong đó Người kiểm tra sẽ thảo luận về các yêu cầu trường hợp và Người yêu cầu và Kỹ thuật viên sẽ đăng ký bằng chứng đã gửi.

Ví dụ, phòng thí nghiệm, phòng thí nghiệm điện thoại di động hoặc phòng máy tính phải được giới hạn cho nhân viên DFL. Mỗi Examiner sẽ yêu cầu một bàn lớn cho thiết bị CNTT, tủ hồ sơ để giữ hồ sơ vụ án và ghế thoải mái. Ngoài ra, bàn phím tiện dụng và thảm có đệm cũng có thể mang lại sự thoải mái hơn cho người kiểm tra.

Nếu DFL yêu cầu máy chủ - điều này có thể được lưu trữ an toàn trong phòng thí nghiệm và nếu có thể, trong một phòng riêng.

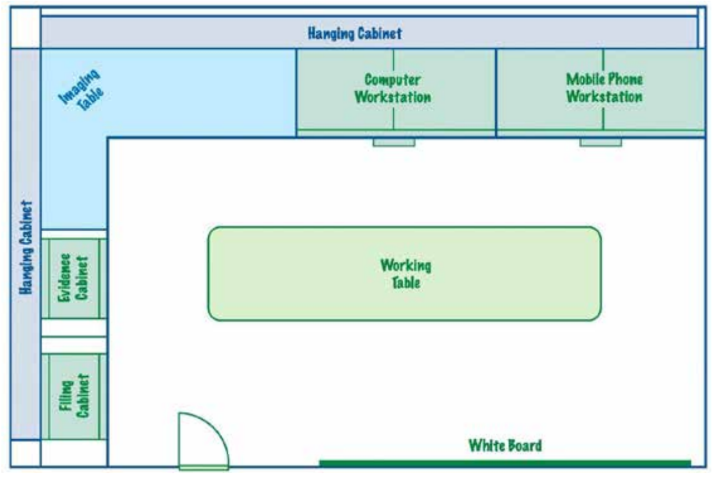
Đó là khuyến cáo để có một khu vực được chỉ định để chụp ảnh và xử lý. Nó nên được tách ra khỏi các máy trạm Examiner và nên ở gần phòng lưu trữ bằng chứng để giảm lượng xử lý thủ công.

DFL cũng có thể xem xét có một không gian để tiến hành các cuộc họp giao ban hoặc các cuộc họp, cũng như một văn phòng bổ sung cho người quản lý phòng thí nghiệm.

Ngoài các khu vực trên, các khu vực dành riêng cho việc lưu trữ các thiết bị phi chứng cứ như máy photocopy, thiết bị sản xuất phương tiện, máy in, máy quét, tập tin, túi tài sản, thẻ, nhãn bằng chứng, phương tiện lưu trữ, thiết bị văn phòng và đồ dùng cá nhân của nhân viên, nên được xem xét khi lựa chọn nơi thích hợp nhất để xác định vị trí phòng thí nghiệm pháp y kỹ thuật số.

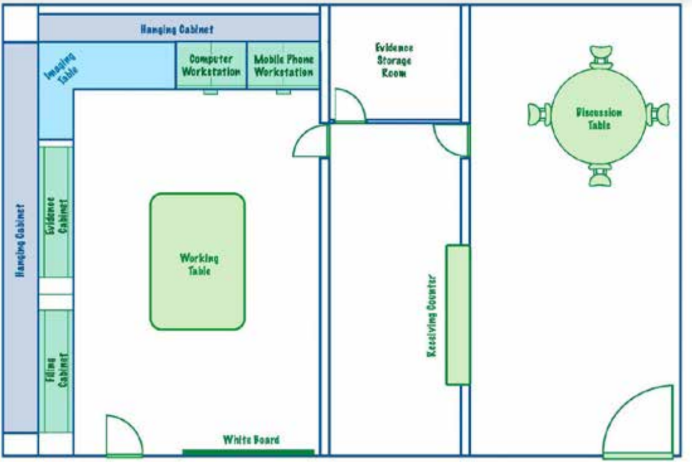
Tòa nhà hoặc văn phòng phải đủ lớn để mở rộng nếu có sự gia tăng dự kiến ​​về công việc DFL. Nhiều DFL hiện tại đã thấy cần phải di dời hoặc mở rộng trong một thời gian ngắn do khối lượng công việc tăng theo cấp số nhân. Nó đắt hơn đáng kể để di dời hoặc mở rộng, vì vậy có thể có ích để cung cấp chỗ cho việc mở rộng trong kế hoạch kinh doanh ban đầu.

Sau đây là một gợi ý cho kế hoạch sàn cơ bản cho DFL.



**Hình 1**. Sơ đồ tầng cơ bản để thiết lập DFL

Nếu một cơ quan quyết định phát triển một DFL có kích thước vừa phải, sau đây là một gợi ý cho kế hoạch sàn.



**Hình 2**. Sơ đồ mặt bằng cho thiết lập DFL có kích thước vừa phải

*2.4 Cơ sở*

Khi các cơ sở đã được chọn và các tính năng bảo mật đã được cài đặt, Trình quản lý phòng thí nghiệm cần nghĩ đến các phương tiện được cài đặt trong DFL.

Các cơ sở phổ biến được cài đặt trong một DFL như sau.

|  |  |
| --- | --- |
| Tiện nghi chung trong DFL | |
| 1 | Khu tiếp tân  Khu vực cung cấp và thu thập bằng chứng điện tử. Tốt nhất là tách khu vực này khỏi phòng thí nghiệm bằng cửa ra vào. Điều này là để ngăn chặn truy cập trái phép vào các phòng thí nghiệm. |
| 2 | Phòng lưu trữ chứng cứ  Phòng được dành riêng để lưu trữ bằng chứng điện tử. Trong một số DFL, căn phòng này cũng được sử dụng để lưu trữ máy chủ. Quyền truy cập vào phòng phải được giới hạn chỉ cho một số nhân viên DFL. Ngoài ra, nếu chỉ có một vài tang vật, thì một giải pháp hiệu quả về chi phí là có một hộp an toàn hoặc tủ chống cháy để lưu trữ tất cả các bằng chứng điện tử thay vì có một phòng lưu trữ chuyên dụng. |
| 3 | Khu vực xử lý chứng cứ  Một khu vực được chỉ định để tháo gỡ, lắp ráp, dán nhãn và hình ảnh bằng chứng điện tử. Khu vực này nên được tách biệt khỏi các máy trạm Examiner và nên gần phòng lưu trữ bằng chứng để giảm lượng xử lý thủ công. |
| 4 | Phòng thí nghiệm  Tùy thuộc vào các loại trường hợp DF nhận được, một DFL có thể có một số phòng thí nghiệm để phân tách công việc dựa trên các loại bằng chứng. Ví dụ bao gồm Phòng thí nghiệm pháp y máy tính, Phòng thí nghiệm điện thoại di động, Phòng thí nghiệm âm thanh hoặc video. |
| 5 | Không gian cá nhân  Trong một số DFL, nhân viên nên có bàn làm việc riêng để thực hiện các nhiệm vụ hành chính, viết báo cáo và tạo các slide thuyết trình. Các phòng thí nghiệm chỉ được sử dụng cho công việc phân tích, trong khi không gian cá nhân này được nhân viên sử dụng cho các sản phẩm công việc cần thiết khác. |
| 6 | Tóm tắt không gian  Một không gian giao ban là nơi Giám khảo có thể thảo luận về một trường hợp và nơi người quản lý / giám đốc DFL có thể tổ chức một cuộc họp giao ban về một trường hợp. Phòng có thể là một không gian mở hoặc đóng. Thật tốt khi trang bị cho phòng một màn hình hiển thị và bảng trắng để tạo điều kiện thảo luận hoặc thuyết trình. |
| 7 | Truy cập Internet bị cô lập và chưa được lọc  Các phòng thí nghiệm trong DFL thường có mạng riêng biệt từ mạng của tổ chức. Điều này là để ngăn chặn phần mềm độc hại và vi rút xâm nhập vào phần còn lại của mạng.  Hơn nữa, DFL phải có quyền truy cập Internet không giới hạn và chưa được lọc. Một số trường hợp yêu cầu Giám khảo truy cập các trang web giả mạo, vì vậy họ cần có quyền truy cập Internet cho phép thực hiện việc này. Mạng này phải được cung cấp bảo mật và tối thiểu là một hệ thống phát hiện và ghi nhật ký xâm nhập cơ bản cần được theo dõi và bảo trì định kỳ. |

**Bảng 3**. Các phương tiện phổ biến trong DFL

*2.5 Khách*

Quyền truy cập của khách truy cập vào DFL phải được hạn chế để ngăn chặn rò rỉ dữ liệu hoặc bất kỳ thiệt hại nào có thể xảy ra đối với bằng chứng điện tử. Khách truy cập có thể bao gồm nhân viên bảo trì, nhân viên từ các cơ quan khác, chuyên gia tư vấn hoặc người cung cấp bằng chứng điện tử.

|  |  |
| --- | --- |
| Danh sách kiểm tra cho khách truy cập | |
| 1 | Đăng ký  Khách truy cập phải được đăng ký bằng biểu mẫu hoặc qua hệ thống trực tuyến trước khi vào cơ sở DFL. Đối với một nhóm lớn khách truy cập, nhân viên DFL đi kèm phải tổ chức các quy trình đăng ký phù hợp, lưu ý đến cơ quan, quy mô của nhóm và mục đích của chuyến thăm. |
| 2 | Thẻ ID  Thẻ ID tạm thời có thể được cấp cho khách truy cập, đặc biệt đối với các lượt truy cập dài. Thẻ ID phải phân biệt rõ khách truy cập với nhân viên DFL. |
| 3 | Người hộ tống  Khách truy cập phải được nhân viên DFL đồng hành mọi lúc khi ở trong khuôn viên DFL. |
| 4 | Chính sách khách truy cập  Clearsigns hoặc một poster về Chính sách khách truy cập phải được hiển thị trong khu vực chung DFL để khách truy cập đọc. Các quy tắc như chụp ảnh, ăn uống, chạm vào thiết bị pháp y và bằng chứng điện tử, v.v ... phải được nêu rõ cho du khách. Hướng dẫn phải đơn giản và dễ đọc cho người không nói tiếng Anh. |
| 5 | Xem của Contraband  Các dấu hiệu rõ ràng sẽ chỉ ra rằng các hình ảnh bất hợp pháp và không phù hợp đang được phân tích và xem trong DFL. |

**Bảng 4**. Danh sách kiểm tra cho khách truy cập

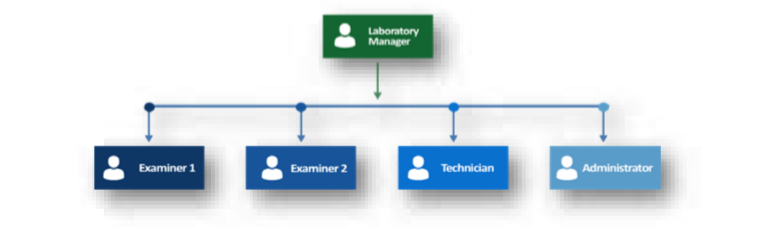


***3 Nhân viên***

Tùy thuộc vào quy mô của phòng thí nghiệm và số lượng nhân viên cần thiết, các chức năng khác nhau đó là bắt buộc phải được xem xét. Vai trò và trách nhiệm của nhân viên sẽ cần được ghi lại. Mô tả công việc chi tiết nên được chuẩn bị để mỗi thành viên trong nhóm có một sự rõ ràng sự hiểu biết về hồ sơ công việc của anh ấy / cô ấy. Khi có thể, cấu trúc của một DFL sẽ cho phép nhân viên thăng tiến nghề nghiệp trong tổ chức. Kinh nghiệm cho thấy rằng các nhân viên có trình độ cao dành phần lớn thời gian của họ để thực hiện các nhiệm vụ trần tục dưới mức độ chuyên môn của họ. Một hồ sơ công việc và một lộ trình nghề nghiệp được đặt ra rõ ràng ở giai đoạn đầu của sự phát triển DFL sẽ cung cấp định hướng cho việc lập kế hoạch và dự báo ngân sách của tổ chức

*3.1**Tuyển dụng*

Nhân viên được tổ chức làm việc cho DF làm việc thường phụ thuộc vào loại trường hợp DF và tổng số bằng chứng điện tử được nộp cho DFL. Những nhân viên này có thể đến từ bất kỳ nền tảng giáo dục, nhưng phải có nền tảng cơ bản mạnh mẽ và sự quan tâm cao trong điện toán lĩnh vực và những tiến bộ hiện tại trong công nghệ. Một DFL thường bao gồm, tối thiểu, một Trình quản lý phòng thí nghiệm và hai Giám khảo. Giám khảo làm việc tại DFL, phân tích bằng chứng điện tử và đôi khi có thể được yêu cầu để đi đến trang web hiện trường để tiến hành bảo quản bằng chứng. Nếu có sự gia tăng trong các trường hợp và nhiều thiết bị pháp y là thu được, thường là tốt nhất cho DFL sử dụng một Kỹ thuật viên. Quản trị viên cũng có thể được tuyển dụng nếu DFL xử lý nhiều nhiệm vụ hành chính như quản lý khác nhau tài liệu, đào tạo, thăm, và nói chuyện. Một sơ đồ tổ chức được đề xuất ở mức tối thiểu như sau:



**Hình 3.** Sơ đồ tổ chức để thiết lập cơ bản Phòng thí nghiệm pháp y kỹ thuật số

*3.2**Giải phóng mặt bằng an ninh*

Trước khi nhân viên DFL được tuyển dụng, các ứng cử viên nên trải qua kiểm tra lý lịch hoặc bảo mật kiểm tra. Tối thiểu, DFL hoặc Phòng Nhân sự phải đảm bảo rằng một ứng cử viên không có tiền án tiền sự và đã được cơ quan chức năng thông qua một cách thỏa đáng. Trong khi những giải phóng mặt bằng có thể không phải lúc nào cũng lý tưởng, ít nhất họ cung cấp một dấu hiệu của bất kỳ tội phạm nghiêm trọng hành vi phạm tội trong quá khứ. Đó là thông lệ cho Phòng Nhân sự hoặc DFL quản lý để có quyền truy cập vào lưới và hồ sơ cá nhân của ứng viên trước khi phỏng vấn quá trình, hoặc ít nhất là trong phiên phỏng vấn.

*3.3**Mô tả công việc*

Tất cả nhân viên phải có Mô tả công việc rõ ràng sau khi được DFL tuyển dụng. Mỗi cá nhân

vai trò và trách nhiệm trong DFL phải được giải thích trong Mô tả công việc. Ở mức tối thiểu,

vai trò và trách nhiệm của từng nhân viên trong DFL cần được giải thích như sau:

**Mô tả về vai trò và trách nhiệm**

**Quản lý phòng thí nghiệm**

Giám đốc phòng thí nghiệm phải có kiến ​​thức kỹ thuật và hiểu biết sâu sắc về yêu cầu lập pháp cho bằng chứng điện tử, thủ tục và quy trình. Phòng thí nghiệm Người quản lý phải hiểu các nguyên tắc bao quát được mô tả trong hướng dẫn này. Anh ấy / Cô ấy phải có quyền kiểm soát đối với thiết lập ban đầu và xây dựng giám sát liên quan đến mua phần cứng và phần mềm hoặc các quy trình và chức năng DFL. Anh ấy / cô ấy chịu trách nhiệm lãnh đạo tuyển dụng, đào tạo, cố vấn, tư vấn và hướng dẫn của mọi người làm việc trong đơn vị. Giám đốc phòng thí nghiệm cũng chịu trách nhiệm ra quyết định liên quan đến các trường hợp cá nhân, bao gồm cả việc có chấp nhận hay không hoặc từ chối một trường hợp cũng như các ưu tiên.

**Giám khảo**

Giám khảo phải có kiến ​​thức kỹ thuật liên quan và bằng cấp phù hợp. Lý tưởng nhất là anh ấy / cô ấy nên được đào tạo về việc sử dụng phần mềm DF.Khi được thuê, Examiner sẽ được yêu cầu tham gia khóa đào tạo cụ thể để có được bộ kỹ năng tối thiểu. Giám khảo phải có kiến ​​thức về pháp luật và nhận thức được các yếu tố của mỗi hành vi phạm tội để làm rõ những sự thật đó khi điều tra các loại tội phạm khác nhau. Những vai trò này đòi hỏi một tư duy phân tích và điều tra. Giám khảo cũng phải có khả năng đưa ra kết quả của mình một cách rõ ràng và dễ hiểu cách, do đó có kỹ năng giao tiếp bằng lời nói và bằng văn bản là rất cần thiết.

**Kỹ thuật viên**

Kỹ thuật viên tiến hành xử lý bằng chứng như đăng ký, mua lại và lưu trữ. Tùy thuộc vào quy mô của phòng thí nghiệm, một số kỹ thuật viên có thể được yêu cầu. Các Kỹ thuật viên phải có kỹ năng kỹ thuật mạnh mẽ trong lĩnh vực máy tính và kỹ thuật kiến thức về các phương pháp khác nhau để thu thập dữ liệu kỹ thuật số. Một kỹ năng quan trọng yêu cầu là chú ý đến chi tiết và khả năng ghi lại rõ ràng tất cả các hành động được thực hiện trên mỗi mục bằng chứng. Kỹ thuật viên cũng chịu trách nhiệm bảo trì thiết bị pháp y. Anh ấy / cô ấy cần phải đảm bảo rằng phần sụn phần cứng được cập nhật và các bản vá và cập nhật phần mềm cài đặt khi phát hành. Kỹ thuật viên cũng chịu trách nhiệm xử lý các bằng chứng trong Kho lưu trữ chứng cứ Phòng. Anh ấy / cô ấy cần phải duy trì hồ sơ bằng chứng cũng như kiểm tra và kiểm tra Triển lãm trong Phòng lưu trữ.

**Người quản lý**

Một DFL cũng có thể sử dụng Quản trị viên để thực hiện các nhiệm vụ hành chính của phòng thí nghiệm. Anh ấy / cô ấy chịu trách nhiệm quản lý các tài liệu, đào tạo và đàm phán DFL. Anh ấy / cô ấy có thể cũng hoạt động như một sĩ quan liên lạc cho các bên liên quan bên trong cũng như bên ngoài. Quản lý hành chính cũng có thể chịu trách nhiệm xử lý việc mua thiết bị cho phòng thí nghiệm

*3.4**Phát triển nhân viên*

Quản lý DFL phải đảm bảo rằng nhân viên tham gia vào các nhiệm vụ DF được trang bị đầy đủ và có kỹ năng phù hợp. Lý do cho điều này là dữ liệu chứa trong bằng chứng điện tử có thể dễ dàng thay đổi, bị hư hỏng hoặc bị phá hủy bởi một lần duy nhất của một phím, vì vậy nhân viên phải biết cách xử lý dữ liệu mà không cần làm hỏng chúng Một lý do khác là sự phức tạp của tội phạm ngày nay có thể gây khó khăn cho khám phá đúng dữ liệu; do đó, nhân viên DFL phải biết cách tìm và trích xuất chúng.

**A. Đào tạo**

Khi nhân viên đã được tuyển dụng, điều quan trọng là liên tục phát triển khả năng của họ để

thúc đẩy và giữ chân họ, và thiết lập một chương trình phát triển nhân viên có thể đạt được hỗ trợ này Điều này nên bắt đầu với một cảm ứng đến nơi làm việc mới của họ. Mô tả công việc phải chỉ rõ vai trò và trách nhiệm của họ và người quản lý báo cáo của họ. Người quản lý phải xác định và lập kế hoạch cho nhu cầu đào tạo nhân viên và sắp xếp phù hợp. Các DFL có thể chọn gửi nhân viên vào các khóa đào tạo hoặc có thể sắp xếp một phiên để nhân viên bóng tối và học hỏi từ các đồng nghiệp, theo một dòng thời gian dự kiến. Ví dụ, tất cả Giám khảo sẽ yêu cầu đào tạo được chứng nhận bên ngoài để cung cấp cho họ sự tự tin để sử dụng các công cụ pháp y và độ tin cậy để cung cấp bằng chứng đáng tin cậy tại tòa án. Một kỹ năng được đề xuất có thể hữu ích trong việc xác định nhu cầu đào tạo có sẵn tại Phụ lục **A: Bộ kỹ năng DFL** **Danh mục.**

**B. Bảo trì thành thạo**

Những tiến bộ trong công nghệ đòi hỏi nhân viên phải thường xuyên được cập nhật với quyền

kiến thức và kỹ năng. Ngoài chương trình đào tạo, DFL nên xem xét việc có một chương trình bảo trì thành thạo, là một phần trong đó nhân viên sẽ được yêu cầu tham dự hội thảo về cập nhật công nghệ, tham dự các cuộc họp liên quan đến kỹ thuật, liên tục tiến hành phân tích bằng chứng điện tử, tham dự các cuộc biểu tình sản phẩm, hoặc tham gia đào tạo lại các chương trình. Chương trình này rất quan trọng để đảm bảo rằng các kỹ năng của Giám khảo được cập nhật với

công nghệ hiện tại và họ luôn có thể thực hiện các nhiệm vụ DF.

**C. Danh mục đầu tư phát triển cá nhân (PDP)**

Để quản lý hiệu quả việc phát triển nhân viên, DFL có thể xem xét ban hành từng thành viên của nhân viên với một danh mục đầu tư phát triển cá nhân (PDP). Danh mục đầu tư này nên có một kế hoạch đào tạo, chứng chỉ đào tạo, hồ sơ tham dự, cũng như hồ sơ về các mốc quan trọng đạt được trong nơi làm việc Người quản lý có thể sử dụng PDP để đặt mục tiêu cho các cá nhân và giám sát họ hiệu suất theo thời gian.

**D. Hoạt động nghiên cứu và phát triển**

Ngoài việc đào tạo và bảo trì thành thạo, quản lý cũng phải dành ra một số thời gian để nhân viên thực hiện các hoạt động nghiên cứu và phát triển. Các nhân viên nên đánh giá các công cụ và ứng dụng mới sắp xuất hiện trên thị trường và quyết định xem có cần thiết cho DFL để sử dụng chúng.

**E. Giữ chân nhân viên**

DFL cần lưu ý rằng chương trình đào tạo mở rộng làm cho nhân viên có giá trị cao đối với

các tổ chức khác để thuê, do đó tỷ lệ doanh thu cao trong DFL. Rất nhiều thời gian và tiền sẽ được dành cho đào tạo nhân viên, và điều quan trọng là họ được giữ lại, đặc biệt là một khi họ trở nên có kinh nghiệm hơn. Để giảm thiểu rủi ro mất nhân viên, Tổ chức nên có một chương trình giữ chân nhân viên tốt tại chỗ. Có kế hoạch phát triển cá nhân mạnh mẽ cho mỗi thành viên của đội ngũ nhân viên sẽ cung cấp cho họ các mục tiêu cá nhân và hiểu rõ hơn về con đường sự nghiệp của họ cũng như các cơ hội trong tương lai trong Tổ chức. Các yếu tố mà đóng góp cho lòng trung thành của nhân viên không phải lúc nào cũng giới hạn ở mức lương; thường là một công việc tốt và lành mạnh môi trường là một yếu tố góp phần.

*3.5**Kèm cặp*

Đối với nhân viên mới được tuyển dụng, nên có một buổi cố vấn trong thời gian thử việc giai đoạn. Kèm cặp là quá trình một nhân viên có kinh nghiệm giám sát người mới được tuyển dụng nhân viên làm việc. Vai trò của người cố vấn là hướng dẫn và hỗ trợ, cũng như chia sẻ thông tin trong một môi trường thân thiện và tự tin. Sự cần thiết cho các buổi cố vấn cho người mới nhân viên được thuê sẽ giảm dần khi họ ổn định vai trò mới của họ. Kèm cặp thường diễn ra cùng với việc thẩm định và đánh giá hiệu suất trong mối quan hệ đến thời gian thử việc.



*3.6**Sức khỏe và an toàn*

Giám đốc DFL chịu trách nhiệm đảm bảo sức khỏe và sự an toàn của tất cả nhân viên và khách đến thăm DFL. Đánh giá rủi ro phải được thực hiện bằng cách kiểm tra bất kỳ điều kiện hiện tại nào trong cơ sở điều đó có khả năng ảnh hưởng đến sức khỏe hoặc sự an toàn. Bất kỳ vật liệu nguy hiểm phải được xử lý. Có thường là một nhân viên hoặc đội ngũ chuyên trách trong cơ quan để chăm sóc các vấn đề sức khỏe và an toàn, nhưng khi không có, người quản lý DFL có trách nhiệm nhận thức được bất kỳ sức khỏe hợp pháp nào và yêu cầu an toàn. Các biện pháp phải được thực hiện để đảm bảo rằng khách và nhân viên từ các bộ phận khác không nhìn thấy hoặc không phải chịu các tài liệu bất hợp pháp hoặc gây phiền nhiễu được tìm thấy trong DFL. Khả năng này có thể là giảm nhẹ bằng cách làm theo các đề xuất được cung cấp trước đây liên quan đến cấu trúc và tập hợp lên DFL. Một số tính năng an toàn phổ biến được tìm thấy trong phòng thí nghiệm điển hình là:

● Thảm chống tĩnh điện và dây đeo cổ tay - để giảm nguy cơ hư hỏng tĩnh cho thiết bị và tang vật.

● Quy định về trang phục - giày dép phù hợp che kín bàn chân phải được mang, tóc dài phải được buộc lại, đồ trang sức và quần áo rộng thùng thình phải được bảo đảm. Nếu cần thiết, găng tay phẫu thuật nên được đeo để tránh tiếp xúc với các chất bị ô nhiễm.

● Xử lý / nâng - đảm bảo nhân viên nhận thức đúng cách để nâng vật nặng để tránh chấn thương.

● Thảm cao su - để giảm nguy cơ bị điện giật.

● Bộ ngắt mạch - để giảm nguy cơ bị điện giật hoặc hư hỏng cho thiết bị và chứng cớ.

***4. Thiết bị***

Một DFL phải có quyền truy cập vào thiết bị pháp y được yêu cầu để tạo ra pháp y chính xác

các kết quả. Thiết bị có thể ở dạng phần cứng, dạng phần mềm, mã nguồn mở hoặc các công cụ thương mại. Trước khi sử dụng, thiết bị phải được kiểm tra và xác minh để đảm bảo có thể sản xuất đúng các kết quả. Thiết bị cơ bản được đề xuất cho DFL có sẵn tại Phụ lục *B: Danh sách kiểm tra của DFL cơ bản Trang thiết bị.*

*4.1**Phần mềm*

Khi mua phần mềm, DFL phải xem xét giá ban đầu, phí giấy phép hàng năm, phí bảo trì và phí đào tạo. Chi phí giấy phép có thể là đáng kể, do đó DFL phải nghiên cứu kỹ lưỡng và bao gồm

điều này trong kế hoạch ngân sách cho các khoản phí hàng năm tiếp theo. Nó phải được đảm bảo rằng phần mềm thu được phù hợp chính xác với các yêu cầu DFL. Một số phần mềm nguồn mở cung cấp các tính năng mở rộng và có thể được Examiners sử dụng, nhưng điều này phần mềm có thể thiếu các cơ hội hỗ trợ và đào tạo. Một số khu vực pháp lý và tiêu chuẩn yêu cầu 'xác minh công cụ kép' và có thể cần phải mua phần mềm bổ sung để tiến hành so sánh và xác minh kết quả. DFL cũng phải xem xét việc có Hệ thống quản lý hồ sơ cho hoạt động của mình. Hệ thống này sẽ giữ cơ sở dữ liệu về các vụ án, tang vật, tên của giám khảo và kết quả pháp y. Các mục tối thiểu cho một hệ thống quản lý trường hợp như sau:

● Ngày, giờ và người giao và nhận triển lãm cho DFL.

● Số tham chiếu triển lãm độc đáo.

● Số tham chiếu trường hợp duy nhất.

● Tên người yêu cầu và chi tiết liên lạc.

● Loại tội phạm và hành vi liên quan.

● Tên của nhân viên DFL đã liên hệ với các cuộc triển lãm.

● Tường thuật cho yêu cầu trường hợp.

● Các yếu tố thời gian - chẳng hạn như ngày giao hàng và ngày ra tòa dự kiến.

● Quá trình phân tích - Hình ảnh, kiểm tra, trích xuất, tính toán giá trị băm, v.v.

● Ngày và thời gian phân tích chính xác được thực hiện, cũng như tên của Người kiểm tra.

● Chi tiết đảm bảo chất lượng của đồng nghiệp và người quản lý.

● Kết quả phân tích.

● Bản ghi liên lạc với Người yêu cầu.

Tất cả thông tin này cực kỳ quan trọng để thể hiện tính liên tục, độ tin cậy và xác minh hành động và bằng chứng. DFL có thể tạo ra hệ thống nội bộ, mua một giải pháp sẵn có hoặc thuê

một lập trình viên để phát triển hệ thống

*4.2**Phần cứng*

Phần cứng cũng phải được bảo trì định kỳ, theo đó khuyến nghị nên có kế hoạch theo lịch trình và một danh sách thiết bị. Một yếu tố quan trọng để DFL xem xét, ngoài việc lưu trữ và sao lưu hoạt động dữ liệu, là lưu trữ các bằng chứng điện tử. Ba loại dữ liệu mà DFL có thể cần phải

đối phó với các bằng chứng ban đầu, các bản sao pháp y và dữ liệu được tạo ra trong quá trình phân tích. Điều cần thiết là DFL phải có một máy chủ lớn, mạnh mẽ và nhanh chóng do khối lượng dữ liệu và bằng chứng điện tử. Phải xem xét cách thức lưu trữ, lưu trữ và sao lưu. Một chế độ sao lưu và lưu trữ nghiêm ngặt nên được thực hiện để mang lại khả năng phục hồi. Danh sách các thiết bị DFL cơ bản có sẵn tại **Phụ lục B: Danh sách kiểm tra Thiết bị DFL cơ bản.**

*4.3**Dụng cụ và phụ kiện*

Các công cụ và phụ kiện như dây cáp, tua vít và bộ mở rộng điện cũng quan trọng như phần mềm và phần cứng trong DFL. Một số công việc DF yêu cầu các thiết bị điện tử phải được tháo rời và được lắp ráp lại, vì vậy DFL cần có quyền truy cập vào các công cụ và phụ kiện chất lượng tốt. Các sau đây là danh sách các mục có thể mà DFL có thể cần để thực hiện các nhiệm vụ hàng ngày:

• Mở rộng nguồn

• Dẫn và bộ điều hợp

• Tua vít

• Bộ công cụ

• Máy ảnh, máy quay video

• Băng từ tính

• Thiết bị liên lạc

• Hộp lưu trữ hoặc hộp đựng thiết bị mang theo

• Đuốc

• Kinh lúp

• Bằng chứng niêm phong hoặc túi bằng chứng

• Dán chống giả

• Điểm đánh dấu vĩnh viễn

• Túi Faraday