3000 series

The Standards of Practice covering 3000 Series, Office of Information Technology Services, are still under review. In the meantime, this document provides relevant guidance for policies and regulations impacting Information Technology Services.

Please note that the linked materials include relevant Board of Education policies, although some policies and numbers may have changed as a result of the Board's update of its policies.

OFFICE OF INFORMATION TECHNOLOGY SERVICES
Standard Practices Series 3000

SP 3000: Office of Information Technology Services; Overview

1. **Purpose**
   To provide an overview of this SP Manual.

2. **Effective**
   Immediately.

3. **Applies to**
   Users of SPs (teachers, school administrators, DOE employees, and personnel in the Office of Information Technology Services).

4. **Mission**
   Fully support the Vision of the Public School Graduate, be the catalyst for innovation, and the provider of choice for information solutions within the DOE.

5. **Vision**
   The DOE will have a "state of the art" information infrastructure which is comprehensive, user-friendly and efficient.

   Organization
   The Office of Information Technology Services is currently composed of three branches:
   1) Information Systems Services branch (ISSB),
   2) Information Resource Management branch (IRMB), and
   3) Network Support Services Branch (NSSB).

   The functions delivered by these branches are listed in the table below.

ISSB	IRMB	NSSB
Technical Development and Support • Student Information Systems • Student Support Systems • Budget Systems • Personnel and Payroll systems • Financial systems • Professional Learning Infrastructure • DOE Website • Data Warehouse • Lotus Notes	Support and Training of DOE-wide Systems • Student Information systems • Student Support Systems • Information Systems Training • Help Desk • Lotus Notes • Data Analysis and Projections • Geographic Exceptions • Federal Impact Aid • FERPA Compliance	Network and Computer Operations • Wide Area Network Operation and Management • School Local Network Installation and Operations Support • School Network and Technical Support • Voice Network • Internet Services • Network Security Services • Video (CATV/CCTV) • Telecom Infrastructure and Electrical CIP • E-Rate Application Process

OITS is the central office for technology in the DOE; however, it works collaboratively with the Office of Curriculum and Instructional Support (OCISS) in many areas regarding technology for students, classrooms, and schools. The use of technology in the classroom for instruction, however, is the responsibility of the Advance Technology Research and the Tele-school branches within OCISS.

6. **SP Maintenance Responsibility**
The Assistant Superintendent in the Office of Information Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) reference page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone.

7. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP 3000

SP 3250: Financial Management System Functions; Description of

1. **Purpose**
To describe the functions of the Financial Management System (FMS).

2. **Effective**
Immediately.

3. **Applies to**
All Department of Education employees involved in financial, purchasing, and fixed assets functions.

4. **Description**
A. FMS is the DOE's accounting and financial management system. It is used by all DOE schools and offices and provides multi-level organizational security.

B. The client software known as WINFMS is distributed over the internet accessible only through the DOE's network. The software features a graphical user interface w/pull-down menus and provides added security and error checking functions.

FMS uses within the schools, state, complex, and district offices include:
1) Plan Adjustments,
2) Allotment Status Monitoring,
3) Purchasing,
4) Cash Receipts and Deposits,
5) Fixed Assets,
6) Payments,

7) Payment and Receipt Adjustments, and
8) Inquiries and Reports.

C. FMS functions are unique to the Central Accounting, Vendor Payments, and Procurement offices in the following areas:
1) Check Writing,
2) Contract Writing,
3) Vouchers,
4) Project and Grant Accounting,
5) Journal Table Maintenance, and
6) Interfaces To/From Other Systems.

5. **Hardware Requirements**

PC-compatible Computer capable of running Microsoft Windows 2000 or XP Operating System includes:

A. 450 MHz or higher processor clock speed – Intel Pentium/Celeron family, AMD K6/Athlon/Duron family, or compatible processor recommended,
B. 256MB RAM (memory) or higher,
C. 10GB hard drive or larger,
D. 8MB or larger Video Card,
E. 10/100 Network interface card,
F. Keyboard and Microsoft Mouse or compatible pointing device, and
G. Network Laser Printer.

6. **Software Requirements**

Microsoft Windows 2000 or XP Operating System
Microsoft Internet Explorer v5.x and higher (IE5.x)
WINFMS Software
Cisco VPN Client
Timbuktu Pro for Windows

7. **SP Maintenance Responsibility**

The Financial Systems Data Processing Specialist of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below.

8. **References, Resources, and Forms**

The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP3250
(b) FMS Web Site

SP 3251: Financial Management System

1. **Purpose**

To download software for access to the Financial Management System (FMS).

2. **Effective**
Immediately.

3. **Applies to**
All DOE employees involved in financial, purchasing, and fixed assets functions.

4. **Process**
A. Access the DOE Windows Software Site using Internet Explorer v5.x or higher. See Reference (b).

B. Print Appendix C – WINFMS: Schools/Offices Installation Checklist available by clicking on the Read Me First link. Follow the steps listed in the checklist. See Reference (b).

C. Use FMS-required software, which is available at the Software Download Center on the DOE Windows Software Site. See Reference (c).
1) WINFMS Software
2) Cisco VPN Client Software
3) Timbuktu Pro for Windows

5. **SP Maintenance Responsibility**
The Financial Systems Data Processing Specialist of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below.

6. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP3251
(b) FMS Web Site
(c) DOE ISSB Windows Software Site

Forms
(d) Appendix C – WINFMS: Schools/Offices Installation Checklist

SP 3252: Financial Management System; Procedure to Access

1. **Purpose**
To request a Financial Management System (FMS) user sign on.

2. **Effective**
Immediately.

3. **Applies to**
All DOE employees involved in financial, purchasing, and fixed assets functions.

4. **Process**
A. Access the FMS Forms Web page using Internet Explorer v5.x or higher. See Reference (b).
B. Click on the FMS-AT1 - Security Change Request Form link. See Reference (c).
C. Complete the form and print it.
D. Fax the completed form to ISSB-Financial and Budget Systems (692-7752).

5. **Software Requirements**
Microsoft Windows 2000 or XP Operating System
Microsoft Internet Explorer v5.x and higher (IE5.x)
Adobe Reader – Download the latest version of Adobe Reader

6. **SP Maintenance Responsibility**
The Financial Systems Data Processing Specialist of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP 3252 may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below.

7. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP 3252
(b) FMS Web Site

8. **Forms**
(c) FMS-AT1 - Security Change Request Form

SP 3255: Budget System; Procedure to Access

1. **Purpose**
To describe the procedure to access the Budget System.

2. **Effective**
Immediately.

3. **Applies to**
School Administrative Services Assistants and/or Account Clerks, District Office Secretaries, and State Office Secretaries.

4. **Background**
General, Federal, and Special Funds in the DOE's budget system are transferred to the DOE's Financial Management System (FMS) for purchases, receivables, and payments. To ensure the security of the Budget System, users must gain access through a username and password, which should be periodically changed.

5. **User's Login Account Creation/Password Change/Retrieval**
Each Organization ID is assigned a username and password. Passwords can be changed in the Budget System. Passwords can be reset by completing a Password Change Request. See Reference (d).

6. **Special Requirements**
HyperAccess must be installed on a Microsoft Windows 9x, 2000, XP Operating System or higher. Please see the Instructions for Budget HyperAccess for Windows for more information. See Reference (c).

7. **SP Maintenance Responsibility**
The Budget Systems & Special Application Development section leader of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See **Reference (a)** below**.**

8. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP 3255
(b) Forms, and Procedures website
(c) Instructions for Budget HyperAccess for Windows website
(d) Password Change Request website

SP 3260: Casual Payroll System; Procedure to Access

1. **Purpose**
To describe the procedure to access the Casual Payroll System.

2. **Effective**
Immediately.

3. **Applies to**
School Administrative Services Assistants, Clerks, Secretaries, Timekeepers, and other staff responsible for the tracking of employee hours worked and for maintaining leave records.

4. **Background**
The Casual Payroll System provides Time and Attendance functions for the Department's Casual Personnel employees, including those in special categories such as Emergency Hire employees, Student Helpers, Teachers who are paid stipends, etc. For each semi-monthly pay period, the user enters the date and hours an employee works at a specific position. The system then calculates the proper pay for the

employee and submits the payroll records for payment to the employee within the DOE pay cycles.

5. **Users Login Account Creation/Password Change/Retrieval**
To access the Casual Payroll System requires a username and password. Each Org ID is assigned a username and password, and can optionally request an additional Casual Payroll Account by completing a Casual Payroll Account Request. See Reference (d) below. In the Casual Payroll System, passwords can be changed or reset by completing a Password Change Request. See Reference (e) below.

6. **Special Requirements**
Hyper Access must be installed on a Microsoft Windows 9x, 2000, XP Operating System or higher. Please see the Instructions for Budget Hyper Access for Windows or Reference (c), for more information.

7. **SP Maintenance Responsibility**
The Budget Systems & Special Application Development section leader of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) reference page for this SP may provide standard responses to common questions. It is available on the Casual Payroll Website. Please review this resource before inquiring via telephone. See Reference (b) below.

8. **References, Resources, and Forms**
The following resources may provide access to related memos, procedures, and forms. Click anywhere below to access the linked page.
(a) Frequently Asked Questions (FAQ) for SP 3260
(b) Casual Payroll Website
(c) Instructions for Budget HyperAccess for Windows

Forms
(d) Casual Payroll Account Request
(e) Password Change Request

SP 3265: Local School Non-Appropriated Fund Accounting; Procedure to Access

1. **Purpose**
To describe the procedure to access the Local School Non-Appropriated Fund Accounting system. (For convenience, this system hence will be referred to as the "Local School Accounting System".)

2. **Effective**
Immediately.

3. **Applies to**

Principals, Administrative Users, School Administrative Services Assistants, Account Clerks.

4. **Background**

A. **The Local School Accounting System** provides a means for accounting for non-appropriated funds.

B. **Non-appropriated funds**, also known as local school funds, are those monies collected and maintained by the school.

C. **The School is the custodian for all monies collected** from students and/or other sources.

1) Non-appropriated fund sources may include monies raised from fundraisers, athletic booklets, yearbooks, etc.
2) These monies do not require deposit into the State Treasury as authorized under Section 302A-1130 Hawaii Revised Statutes.

D. **Local School Account transactions use the "cash basis"** of accounting. Under the cash basis of accounting, revenue is recognized (recorded or posted) when cash is received, and expenditures are recognized when paid.

E**. Principal's Responsibility:**

The Principal of the school serves as trustee of the non-appropriated local school funds, and is directly responsible for the conduct of school financial activities in accordance with the rules, policies and procedures set forth by the department.

F. **Summary of System Operation**

The Local School Accounting System is an on-line web application, accessible through the use of an Internet browser (Internet Explorer 5.5 and above). No software installation is required for school PCs. Data is stored on a central DOE server. The system provides a means for Quarterly reporting to Central Accounting, which is necessary to meet Department of Accounting and General Services requirements.

G. Other useful information regarding the handling of Local School Accounts can be accessed at the Office of Fiscal Services (OFS) Local School Accounts instructional website. See reference (e).

5. **User Login Account Creation/Password Change/Retrieval**

User ID and passwords used for DOE's Financial Management System (FMS) are also used for the Local School Accounting System. Changing passwords or retrieving of forgotten passwords should follow the procedures for FMS SP 3252.

6. **Special Requirements**

Microsoft Windows 9x, 2000, XP Operating System
Microsoft Internet Explorer v5.x and higher (IE5.x)

7. **SP Maintenance Responsibility**
The FMS Workstation & Web Services Development section leader of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below.

8. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP 3365
(b) HRS Section 302A-1130
(c) Application Web Login URL
(d) Additional Requirements and Website Tips URL
(e) OSF Local School Funds Instructional Website URL
(f) SP 3252 Procedures to Access FMS

SP 3270: Time & Attendance System; Procedure to Access

1. **Purpose**
To describe the procedure to access the Time & Attendance System.

2. **Effective**
January 1, 2006.

3. **Applies to**
Timekeepers (School Administrative Services Assistants, Clerks, Secretaries, and other staff) responsible for the tracking of employee hours worked and maintaining leave records at Schools, District Offices, and State Offices.

4. **Users Login Account Creation/Password Change/Retrieval**
Each T&A user is assigned a username and password after they have completed the required Timekeeper training. Modifications to exiting user sign ons can be requested by completing the Additional Sign On Request form. Time & Attendance Passwords can be reset by contacting the Centralized Services Desk at (808) 377-8320.

5. **Special Requirements**
Microsoft Windows 98, 2000, XP Operating System or higher.
Microsoft Internet Explorer v5.x SP2 or higher.
Adobe Reader – Download the latest version of Adobe Reader See Reference (c).

6. **SP Maintenance Responsibility**
The designated Time & Attendance Project Manager in the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP. To request assistance or to suggest improvements, please send email to TnA_Admin@notes.k12.hi.us

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below**.**

7. **References, Resources, and Forms**

The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.

(a) Frequently Asked Questions (FAQ) for SP 3270
(b) Time & Attendance Bulletin Board
(c) Download the latest version of Adobe Reader

Forms;

(d) Time & Attendance Forms Additional Sign On Request *(T&A Forms Link on Time and Attendance Bulletin Board)*

SP 3275: VAX Student Information System Functions

1. **Purpose**

To describe the functions of the VAX Student Information System.

2. **Effective**

Immediate.

3. **Applies to**

All DOE employees involved with enrolling students and/or updating and reporting Student data in Hawaii public schools.

4. **Description**

The VAX Student Information System consolidates student demographic data from DOE and Public Charter School computer systems. Access and update is accomplished by on-line Telnet terminal sessions and automated processing of files received from other DOE systems. Functions include:

A. Student demographic information including school, enrollment status, home & mailing address, contact information, and eligibility for support services.
B. On-line access for school personnel and State/District Level personnel to search, view and maintain student information.
C. Reporting of data upload errors, school roster, next school year roster, free and reduced meals, non-disclosure, ELL rosters.
D. Data collection and distribution of student demographic, free and reduced meal, and student services data.

5. **SP Maintenance Responsibility**

The School & Student Systems Development section supervisor, in the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone.

6. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities as well as closely related SPs, procedures, and forms.

SP 3280: Posting Information on the DOE Website

1. **Purpose**
The purpose of this memorandum is to outline the procedure for requesting information to be posted on the DOE web site.

2. **Effective**
Upon approval.

3. **Applies to**
This memorandum applies to any office/person wishing to post information on the department web site.

4. **Procedures**

A. Who may submit requests?
   1) Any manager at the director level or above may submit posting requests to the DOE webmaster.
   2) Directors (or above) may designate, in writing, individuals authorized to submit certain types of information.

B. How to submit requests:
   1) Requests may be submitted via email to the webmaster@k12.hi.us. Requests will not be accepted from non-DOE email addresses.
   2) Submit content to the webmaster in electronic form. Preferred formats are Microsoft Word and Microsoft Excel. Most other common document formats, except page layout programs (e.g. PageMaker, QuarkExpress), are probably acceptable, but please check with the webmaster before sending materials. Microsoft Office documents saved in HTML format will not be accepted.
   3) Information/content submitted as Adobe Acrobat (PDF), audio, or video files, must also include a Microsoft Word (.doc) or plain text document (.txt) with content equivalent to the file or an explanation of why it cannot be provided.
   4) Requestors should include descriptions of images that contain information that adds to or reinforces information in the text. For example, a picture showing proper ergonomic seating of a person in front of a computer may need to describe desired wrist/arm position and monitor viewing angle.
   5) Requestors should describe the target audience, purpose, or other information that will help in appropriate placement of the information.

Requestors should specify if content needs to be password-protected or limited to DOE users only to enable workgroups, etc.

6) Requestors should include a short (one or two sentence) introductory paragraph for a new topic expected to require a separate page.

7) Requestors should provide a date that the information should be removed if the information will expire, e.g. surveys, contests with established deadlines.

8) The requestor is responsible for:
   - **a.** Coordinating with other affected offices.
   - **b.** Weighing the benefit of linking to commercial web sites. Links will be presented in a manner that does not appear to inordinately endorse the company and/or product.
   - **c.** Obtaining and maintaining proof of permission/releases for content included in the posting. For example, this might apply to images taken from another web site, or photos of students requiring parental permission.
   - **d.** Reviewing the posted information after being notified of its completion to make sure it is posted correctly and informing the webmaster of any problems.
   - **e.** Answering subsequent ADA-related complaints/inquiries if equivalent text is not provided with PDF, video, photo, audio, and other non-text submissions.
   - **f.** Periodically reviewing the information, and providing timely updates and/or instructing the webmaster when the material may be removed. If the requestor informs the webmaster when the information is posted of the expected removal date, the webmaster can schedule its automatic removal.

5. **SP Maintenance Responsibility**

The department webmaster in the Information System Services Branch of OITS is responsible for maintenance and questions regarding this SP document.

6. **References and Resources**

None

SP 3282: Website Accessibility Compliance

1. **Purpose**

The purpose of this memorandum is to outline the procedure for insuring 508 accessibility of school web sites.

2. **Effective**

Upon approval by the ITQC.

3. **Applies to**

This memorandum applies to web sites in the department.

4, **Background**

The Americans with Disabilities Act (ADA) and the Rehabilitation Act of 1973 require that state and local governments insure that their web sites are accessible to people with disabilities.

5. **Responsibilities**

Web sites within the department have an obligation to be accessible to all who attempt to use it.

a. If an individual, group, school or office staff develops a web site, the site's webmaster and principal/supervisor need to be sure that the site meets accessibility standards. A good guide to use is the Section 508 standards. The web site webmaster will perform periodic checks/repairs of pages to insure that pages meet accessibility standards. If the site cannot meet these standards, the school/office should immediately block the non-compliant pages from public view until the pages are brought up to standard.

b. Each web page will contain a phone number (including identification of "via relay") and/or email address for the web site's webmaster, and list the school/office responsible for the web site. If there is a complaint against the web site and the contact information is not listed and/or the owner cannot be identified the site may be blocked from public view by OITS.

6. **SP Maintenance Responsibility**

The departmental webmaster in the Office of Information Technology Services is responsible for maintenance of and questions regarding this SP document.

The Frequently Asked Questions (FAQ) for this SP provides standard responses to common questions. **Please "click" Reference (a) below.**

7. **References and Resources**

(a) Frequently Asked Questions (FAQ) for SP 3282 (on-line)
(b) Federal Access Board Section 508 guide

SP 3285: Database for English Language Learners; Access Request Procedure

1. **Purpose**

Describe procedures to access the Database for English Language Learners (DELLS) application.

2. **Effective**

Immediately.

3. **Applies to**

English Language Learners (ELL) Teachers and authorized school personnel, ELL District Resource Teachers, ELL Administrators and staff.

4. **Background**

The DELLS application is administered by the ELL program staff of OCISS.

5. **User Access**
   A. A DOE Lotus Notes account is required for access.
   B. After establishment of a Lotus Notes account, submit DELLS access request through the ELL District Resource Teacher (RT). OCISS ELL Program staff will process the request.
      1) Honolulu District RT, call **(808) 733-4768**
      2) Central District RT, call **(808) 622-6420**
      3) Leeward District RT, call **(808) 675-0443**
      4) Windward District RT, call **(808) 233-5715**
      5) South Hilo RT, call **(808) 933-0367**
      6) North Hilo RT, call **(808) 974-4656**
      7) West Hawai'i RT, call **(808) 323-4555**
      8) Maui District RT, call **(808) 873-3951**
      9) Kauai District RT, call **(808) 274-3509**

6. **SP Maintenance Responsibility**
   The School and Student Systems section head of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

7. **References, Resources, and Forms**
   The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.

SP 3290: Student Priority Ranking Database for NCLB School Choice

1. **Purpose**
   To describe the functions of the No Child Left Behind Student Test Scores application.

2. **Effective**
   Immediately.

3. **Applies to**
   Staff assigned to maintain the data in this application and/or involved in the process of granting School Choice and Supplemental Educational Services (SES) to the lowest achieving low-income students.

4. **Description**
   The NCLB Student Test Scores application assists schools in identifying and prioritizing students for School Choice and SES. The priority rank is determined by (1) free/reduced lunch eligibility, (2) mathematics grades, and (3) language arts grades.

   Features include:
   A. Access through a web browser;
   B. School assigned login;

C. Student roster by semester with mathematics and language arts grades, Free/Reduced Lunch eligibility, Section 504 eligibility, SPED eligibility, and English Language Learner eligibility;
D. Daily update of student demographic data from Vax SIS for student school, name, grade level, lunch status, sped status, 504 status, ELL status;
E. Calculation of a priority rank value between 0 through 10;
F. Data Entry for schools to maintain up-to-date student information;
G. Access to student roster of prior semesters;
H. Export of student roster to Excel file; and
I. Complex Area and Statewide Summary Reports.

5. **SP Maintenance Responsibility**
The School & Student Systems Development section head of ISSB is responsible for maintenance, administration, and questions regarding this SP.

6. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities as well as closely related SPs, procedures, and forms.
(a) NCLB Priority Ranking Website

SP 3310: VAX/IBM Computer Personnel/Payroll Systems; Description of

1. **Purpose**
To store, process, and report personnel/payroll information.

2. **Effective**
Immediately.

3. **Applies to**
Educational Officers, Personnel Management Specialists, Teachers and Substitute Teachers, Office of Business Services (OBS) Payroll Claims Supervisor and Payroll Clerks, Personnel Technicians and Clerks, School Registrars, School Administrative Services Assistants (SASA), Personnel Regional Officers, and Office Secretaries.

4. **User Login Account Creation/Password Change/Retrieval**
A. Supervising Educational Officer/Manager requests Information Systems Services Branch (ISSB)/Network Support Services Branch (NSSB) for VAX computer user account and/or IBM Time Sharing Option (TSO) account.
B. ISSB assigns appropriate VAX computer login menu procedure to user account.
C. NSSB creates VAX computer user account and/or ISSB has Information and Communication Services Division (ICSD) assign IBM TSO account.
D. NSSB notifies user that VAX computer user account is active and/or ISSB notifies user that ICSD TSO account is active.

5. **Special Requirements**
QVT, HyperAccess, or other VAX VT220 emulation software must be installed on a Microsoft Windows 9x, 2000, XP Operating System or higher.

6. **SP Maintenance Responsibility**
The Personnel and Payroll Systems Development section leader of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below**.**

7. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP 3310

SP 3315: Worker's Compensation System; Description of

1. **Purpose**
To store, process, and report Worker's Compensation information.

2. **Effective**
Immediately.

3. **Applies to**
OHR Personnel Management Specialists and Clerks.

4. **User Login Account Creation/Password Change/Retrieval**
A. Supervising Educational Officer/Manager requests from Information System Services Branch (ISSB) a Worker's Compensation System user account.
B. ISSB creates Worker's Compensation System user account with appropriate role privileges.
C. ISSB notifies user that Worker's Compensation System user account is active.

5. **Special Requirements**
Worker's Compensation Renaissance client software and Crystal Reports must be installed on a Microsoft Windows 9x, 2000, XP Operating System or higher.

6. **SP Maintenance Responsibility**
The Personnel and Payroll Systems Development section leader of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) reference page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below**.**

7. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual provisions, and closely related SPs, procedures and forms.
(a) Frequently Asked Questions (FAQ) for SP 3315

SP 3320: Casual Personnel System; Procedures to Access

1. **Purpose**
   To access the Casual Personnel System (CPS).

2. **Effective**
   Immediately.

3. **Applies to**
   CPS Users at Schools, District Offices, and State Offices.

4. **User Login Account Creation/Password Change/Retrieval**
   Each Org ID is assigned a username and password, and it is usually the same one used for Casual Payroll. In the future, users may optionally request an additional Casual Payroll Account by completing a Casual Payroll Account Request. **See Reference (d).** To ensure the security of the Casual Personnel System, users must gain access through a username and password, which should be periodically changed. Passwords can be changed in the System. Passwords can be reset by completing a Password Change Request.

5. **Special Requirements**
   Hyper Access must be installed on a Microsoft Windows 9x, 2000, XP Operating System or higher. Please see the Instructions for Budget Hyper Access for Windows. **See Reference (c)** for more information.

6. **SP Maintenance Responsibility**
   The Personnel & Payroll Systems Development section leader of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.
   The Frequently Asked Questions (FAQ) reference page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See **Reference (a)** below.

7. **References, Resources, and Forms**
   The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
   (a) Frequently Asked Questions (FAQ) for SP 3320
   (b) Casual Personnel Website
   (c) Instructions for Budget Hyper Access for Windows

8. **Forms**
   (d) Casual Payroll Account Request (in the future, cannot be used yet)
   (e) Password Change Request

SP 3335: Empowerosity School Website Content Management System; Procedures to Access

1. **Purpose**
   To access the Empowerosity School Website Content Management System.

2. **Effective**
   Immediately.

3. **Applies to**
   Complex Area Tech Coordinators, School Tech Coordinators, Teachers, and Site Administrator.

4. **Description**
   Empowerosity School Website Content Management System is a vendor application hosted on OITS servers. The application was created for the purpose of providing content managed websites for all DOE schools. It contains, for each school, a website and a content management portal. The portal allows each school to add, delete, or edit web pages containing pictures, text, and hyperlinks. The site access is structured by complex area. Site administrators at each school currently use the system to post school information and reports including the Standards Implementation and Action Plan (SIAP) and Standards Implementation Design (SID), with the Complex Area Supervisors (CAS) having the ability to oversee the process from the website.

   Support issues are handled by the vendor, Empowerosity, through the site's 'Issue Tracker.' See Resource (d). Once logged in as admin, go to 'Other Resources' on the menu and select 'Issue Tracker' to enter or check status of any support issues.

   The Empowerosity Online Help pages on the website may provide standard responses to common questions. Once logged in as admin, Online Help is available from the menu by clicking Help. Please review this resource. See Resource (d) before requesting assistance from your Complex Area Tech Coordinator.

   Empowerosity URL directly to a school website: (replace xxx with the school site id number in the URL below) http://power2.k12.hi.us/index.cfm?siteid=xxx

5. **Users Login Account Creation/Password Change/Retrieval**
   Logins and passwords are distributed by the Complex Area Tech Coordinator for your school. Sub-logins and passwords may be created by each school's Tech Coordinator who administers the school web site. See Resource (b). For additional support, user IDs, and passwords, Complex Area Tech Coordinators may contact OTIS/ISSB at (808) 692-7740 or (808) 586-3200.

6. **Special Requirements**
   Microsoft Windows 9x, 2000, XP Operating System or MAC 9.0 or higher
   Microsoft Internet Explorer v5.x and higher (IE5.x)

7. **SP Maintenance Responsibility**

The FMS Desktop/Workstation & Web Service Development section head in the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) reference page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See Reference (a) below**.**

8. **References, Resources, and Forms**

The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms. Click anywhere below to access the linked page.

(a) Frequently Asked Questions (FAQ) for SP3335
(b) Empowerosity School Websites Home Page URL
(c) School Website Content Management Administration Login URL
(d) Overview of Empowerosity School Websites Content Management System URL

SP 3345: Professional Development Support Center; Access to Web Application

1. **Purpose**

To access the Professional Development Support Center (PDSC) Online Web application.

2. **Effective**

Immediately.

3. **Applies to**

Complex Area Superintendents, Principals, Teachers, DOE Sponsors, Outside Providers, Site Administrators.

4. **Background**

In April 1999, the DOE published the Comprehensive Needs Assessment Report, which highlighted the DOE's need for sustained support for time, resources, and professional development for all educators. The Professional Development Support Center (PDSC) creates the DOE's vehicle for professional inquiry that institutionalizes best practices in education and standards for educators and students. In order for students to achieve, teachers must be competent and qualified to teach, and administrators must be able to organize and lead their schools to support the work of teachers and provide for their growth.

Professional development support is provided in three areas: Teacher Development, Administrative Development, and Systemic Development. PDSC also facilitates adoption of local and national, "cutting-edge" research and development that promote student achievement.

Teacher Development

The program for teacher development:

A. Encourages potential candidates into the teaching profession.
B. Provides support for beginning and in-service teachers in learning and implementing effective research-based strategies that lead to high student achievement in meeting the standards, and
C. Provides for the development of teacher leaders.
D. Builds the leadership capacity of educational administrators to successfully implement the policies of the BOE and the vision of the State Superintendent. PDSC also creates an institutional workplace where administrators, along with their school teams, can gain new knowledge and support the improvement of the schools, which results in promoting high student achievement.

5. **Users Login Account Creation/Password Change/Retrieval**

Creating or changing User Profile information is done by a self registration web link. Changing or retrieving forgotten passwords can also be done using the same web link. See Resource (b) below.

6. **Special Requirements**

Microsoft Windows 9x, 2000, XP Operating System or MAC 9.0 or higher
Microsoft Internet Explorer v5.x and higher (IE5.x).

7. **SP Maintenance Responsibility**

The FMS Desktop/Workstation & Web Service Development section leader of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. **See Reference (a)** below.

8. **References, Resources, and Forms**

The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.

(a) Frequently Asked Questions (FAQ) for SP 3345
(b) Application Web Login URL
(c) Online Help URL
(d) PDSC Website Home Page URL
(e) Overview of Institute URL

SP 3350: Pathways to Leadership Web Application; Access to

1. **Purpose**

To access the Pathways to Leadership (PTL) Online Web application.

2. **Effective**

Immediately.

3. **Applies to**
Complex Area Superintendents, Principals, Teachers, DOE Sponsors, Outside Providers, Site Administrators.

4. **Background**
Pathways to Leadership (PTL) is a Microsoft ASP.NET web application developed for the purpose of creation, registration, and tracking of leadership training events for DOE educational officers (EOs). Leadership training events are created and maintained by system administrators through the administration portal. EOs may log on to the website and register themselves and their leadership team for events. The training completion results are retained in the system. Users may view their registrations and transcripts in their profiles on the website. For an Overview of PTL see Resource (c) below.

5. **Users Log-in Account Creation/Password Change/Retrieval**
To access the PTL, a user will need an Internet-capable computer, and a Lotus Note Account for identity verification. The User must go to the website and create a Password protected user Profile. The User Profile retains all user information related to a registration and transcripts. Changing or retrieving forgotten passwords may also be done on the website.

6. **Special Requirements**
Microsoft Windows 9x, 2000, XP Operating System or MAC 9.0 or higher
Microsoft Internet Explorer v5.x and higher (IE5.x).

7. **SP Maintenance Responsibility**
The FMS Desktop/Workstation & Web Service Development section head of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring for help from the PDERI Office at (808) 832-3201. **See Reference (a)** below**.**

8. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities as well as closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP 3350
(b) PTL Application Home Page URL
(c) Overview of Institute URL

SP 3355: A+ Employee Management System Web Application; Access to

1. **Purpose**
To describe the procedure to access the A+ Employee Management System **(**APLUSWEB) Online Web application.

2. **Effective**
Immediately.

3. **Applies to**
A+ School Clerks, A+ Outside Care Providers, A+ District Coordinators, Dept. of Human Services (DHS) Administrators, A+ Office (OCISS) Administrators, Site Administrators.

4. **Background**
The A+ Employee Management System (APLUSWEB) is an online web application created primarily for the daily management of employee data. The A+ Program and APLUSWEB are administered by OCISS. Access to data is restricted by the role or job function assigned to the user's login. Logins are assigned to A+ Program administrators, A+ Program school clerks, administrators for A+ Program's outside care providers, and DHS administrators who work with the A+ Program. Once logged into the application, click Help on menu for an Overview of APLUSWEB. See Resource (b) below.

5. **Users Login Account Creation/Password Change/Retrieval**
To gain access to the APLUSWEB site, a user must have a per-defined user ID and password. User ID and passwords, as well as forgotten passwords, are obtained by contacting your local A+ District Coordinator. The Center login application is used for site access. Changing passwords is also enabled through Center login.

6. **Special Requirements**
Microsoft Windows 9x, 2000, XP Operating System or MAC 9.0 or higher
Microsoft Internet Explorer v5.x and higher (IE5.x).

7. **SP Maintenance Responsibility**
The FMS Desktop/Workstation & Web Services Development section head of the Information System Services Branch of the Office of Information and Technology Services is responsible for maintenance, administration, and questions regarding this SP. For additional support, A+ District Coordinators or A+ Outside Care Providers may contact the A+ Office at OCISS (808) 842-9845.

The A+ Online Help pages on the website may provide useful responses to common questions. Please review this resource (See Resource (b) below before requesting help from your local A+ District Coordinator.

8. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities as well as closely related SPs, procedures, and forms. Click anywhere below to access the linked page.
(a) Frequently Asked Questions (FAQ) for SP 3355
(b) Application Web Login URL

SP 3360: Textbook Replacement Plan Web Application; Access to

1. **Purpose**
To access the Textbook Replacement Plan Online Web application.

2. **Effective**
Immediately.

3. **Applies to**
Complex Area Superintendents, Assistant Superintendents, Principals, other School Personnel. The public also can view the data without a password.

4. **Background**
The Textbook Replacement Planner is designed to provide schools with an online venue to plan and budget their textbook replacement strategies over a three-year period. This system provides support for the BOE Policy on Instructional Materials, which states:

Schools shall develop and implement a multi-year textbook acquisition/replacement plan that is based on instructional needs. Schools shall inform parents and make available to their school communities the textbook acquisition/replacement plan, its adequacy for meeting students' needs for textbooks in a given school year, and the textbook series by subjects used in the classrooms.

5. **Users Login Account Creation/Password Change/Retrieval**
All accounts to access each school's Textbook Replacement Plan have been created. Changing passwords can also be done using the same web link. **See Resource (a)** below. For the retrieval of forgotten password please contact the help desk at (808) 733-9150.

6. **Special Requirements**
A Microsoft Windows 9x, 2000, XP Operating System and Microsoft Internet Explorer v5.5 or higher.
B MAC OS 9.2 or higher and Microsoft Internet Explorer v5.X or higher.

7. **SP Maintenance Responsibility**
The FMS Desktop/Workstation & Web Services Development section head of OTIS/ISSB is responsible for maintenance, administration and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review it before calling for Help Desk Support at (808) 733-9150.

8. **References, Resources, and Forms**
The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions (FAQ) for SP3360
(b) Application Web Login URL
(c) Textbook Replacement Public Access web link

SP 3710: Department of Education Acceptable Use of Lotus Notes Groupware

1. **Purpose**
   To provide guidelines for the acceptable use (AU) of the DOE's Lotus Notes groupware application, hereby referred to as "LN."

2. **Effective**
   Immediately.

3. **Applies To**
   To all Hawaii Department of Education (DOE) employees, volunteers, students and authorized non-DOE personnel accessing and using LN. The aforementioned individuals are referred to as "users."

4. **Purpose**
   To assure that all users properly use LN. These guidelines reference the DOE's *2170.1 Internet Access Policy and Regulations*. All users are responsible for using e-mail in an efficient, effective, ethical, professional and lawful manner. Users must follow the same code of conduct expected in any other form of written or face-to-face business communication. The DOE may supplement or modify these guidelines for users in certain roles, with the authorization by the Superintendent, Assistant Superintendent, Complex Area Superintendent, or authorized administrators. These e-mail guidelines complement similar DOE policies and guidelines for instant messaging and Internet use. Please read and follow those policies and guidelines, as well.

5. **DOE Regulations and Guidelines**
   The items below are existing policies and guidelines that all users shall follow.
   A. **2170.1 Internet Access Guidelines**

      1. The Department of Education (DOE) Internet services are designed for DOE K-12 students and employees in support of instruction. The DOE Internet Access Policy refers to all resources and systems that are available through the DOE networks. These systems include a variety of DOE Internet and Intranet services including Lotus Notes and Internet conferencing.

      2. Employees access the Internet and electronic mail systems to complete and enhance their job responsibilities. Students use these systems to access resources to support and enhance classroom instruction.

      3. Every school will have an Internet Acceptable Use Policy (AUP).

      4. The DOE reserves the right to review electronic communications. This reminder will be posted on email and other electronic communications screens and sent out annually: "This system is owned and operated by the Department of Education. Email is not private and is subject to management review."

5. The Department of Education (DOE) prohibits the use of electronic communications for personal purposes not connected to the DOE. Electronic communications and email will be used only for (DOE) business.

6. All messages shall be appropriate for DOE purposes. Offensive messages, including foul, hateful language or racial, religious or sexual slurs are prohibited.

7. All DOE personnel issued accounts must participate in staff development sessions offered by the Department in (1) Telecommunication Overview, (2) Electronic Ethics and User Responsibility, and (3) Internet Policies and Guidelines.

8. Users shall respect the integrity of the DOE telecommunication infrastructure. Unauthorized access to the DOE information systems, including internet or other networked computers, is prohibited.

9. Use shall be consistent with the goals of the DOE. The network can be used to market products and services related to DOE instructional activities. Use of the network for personal profit or gain is prohibited.

10. Participants shall respect the privacy of other users -- shall not access modify, or copy passwords or data belonging to their users. Users will not publish private information on students or staff without permission.

11. Authorized owners of the accounts shall be responsible for all communications from their accounts.

12. Users may not access materials inappropriate to the educational mission and goals of the Department such as -- but not limited to -- pornographic materials, adult entertainment, cult/new age, promotion of illegal drugs, gambling, militancy, information on building bombs, information related to unlawful activities or violence, or files dangerous to the network. All DOE schools must block access to such sites.

13. Users shall respect copyright laws and licensing agreements pertaining to material entered into and obtained via the Department's network.

14. Any user who does not comply with the Internet Access Policy will lose network privileges. Repeated or severe infractions of the Policy may result in termination of access privileges permanently. Unauthorized use of the network, intentional deletion or damage to files and data belonging to other users or copyright violations may be termed theft as defined under DOE Chapter 19, the Hawaii Revised Statutes and Federal laws.

B. **Acceptable User Guidelines – Department of Education Network and Internet Servers**

1. User accounts inactive for three or more months (i.e. no logins or file uploads) will be deleted as they pose a security risk and tie up valuable system resources. Users are responsible for their account(s).

2. Users should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their computer resources. Individual password security is the responsibility of each user.

3. Users are forbidden from using techniques designed to cause damage to, deny access by legitimate users of computers or network components connected to the Internet or result in the loss of the recipient's work.

4. Users shall not use another user's account or password without proper authorization.

5. Users are forbidden from circumventing security measures on school or remote computers and networks.

6. Users shall not down-load, install or run security programs or utilities which reveal weaknesses in the security of a system. For example, the users shall not run password cracking programs on any of the Department's computing systems.

7. Users are prohibited from sending unsolicited, commercial and/or offensive e-mail.

8. Users are prohibited from using any form of electronic media (ex. e- mail or web pages) to harass intimidate or otherwise annoy another person/group.

9. Users shall not make copies of system configuration files (e.g. etc/pass word) for their own, unauthorized personal use or to provide to other people/users for unauthorized uses.

10. Users may post pages that are consistent with the public, non-profit educational mission of the Department of Education and are in compliance with all state and federal laws, including those prohibiting obscenity, defamation or copyright infringement.

11. Use of the Department of Education network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited.

12. Use of the Department of Education network to post, send, or retrieve pornographic material, inappropriate text or graphic files, or files dangerous to the integrity of the network are prohibited.

13. Use of the Department of Education network system in a manner that encumbers system and network resources to the point that usage causes interference with others' services is prohibited.

14. The Department of Education network and computing resources shall not be used for political lobbying.

15. The Department of Education is a non-commercial user of the web and use of the web must remain non-commercial. No personal money-making activity may be conducted through the use of the Department's computing and networking resources.

16. The Department of Education is not responsible or liable for materials in violation. Users are responsible for the content of their postings and obtaining all necessary permissions or licenses for any material used.

17. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

18. Sending or receiving unlawful information via electronic communications; using electronic communications illegally in ways that violate local, state, federal, or international laws or statutes are prohibited.

19. Users shall always cooperate with requests from the system administrators for information about the users' computing activities.

20. Users are requested to report any weaknesses in the Department of this agreement to the proper authorities by contacting Network Support Services Branch by sending electronic mail to nssb@k12.hi.us.

21. The Department of Education reserves the right to investigate and monitor any accounts, servers, or machines suspected of policy violation.

22. The Department of Education reserves the right to disconnect any device that is the source of malicious or suspicious activities without notice until the machine in violation is cleaned or fixed.

23. The Department of Education reserves the right without notice to freeze and delete an account that is engaging in activities that violate the Department of Education's policy or the source of spamming, abusive or malicious activities.

6. **Privacy and Access Termination Guidelines**

A. **Monitoring , Reviewing E-mail, and Privacy**

The DOE maintains the right to monitor and review e-mail activity to ensure compliance with its policy, regulations, and guidelines to fulfill the DOE's responsibilities under the state's *Uniform Information Practice Act (Modified)* (UIPA) and other pertinent state and federal laws. UIPA states that, "All government records are open to the public unless access is restricted or closed by law." Users should have no expectation of privacy. The DOE reserves the right to intercept, monitor, review, and disclose any and all messages composed, sent or received. Monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated DOE employees or designated external entities. Employees designated to review messages may include, but are not limited to, an employee's supervisor or administrator, authorized representatives from the Civil Rights Compliance Office (CRCO), authorized representatives of the Office of Information Technology Services (OITS), or appropriate staff at DOE district or complex offices.

DOE reserves the right to alter, modify, re-route or block the delivery of messages as appropriate. This includes but is not limited to the following:

- rejecting, quarantining or removing attachments and/or malicious code from messages that may pose a threat to HIDOE resources;
- discarding attachments, such as music, that are considered to be of little business value and involve a significant resource cost, unless they are work related;
- rejecting or quarantining messages with suspicious content;
- rejecting or quarantining messages containing offensive language;
- re-routing messages with suspicious content to designated HIDOE employees for manual review; and,
- appending legal disclaimers to messages.

Electronic messages are legally discoverable and permissible as evidence in a court of law. Any content created with the e-mail system is considered the intellectual property of the DOE.

B. **Termination of LN Accounts**

Upon termination or separation from the DOE, the user's e-mail address will be immediately terminated from the Domino Name-Address Book (NAB) and will no longer have access to e-mail, including the ability to download, forward, print or retrieve any message stored in the system.

The employee's supervisor or higher authority can request for that employee to access their mailbox for a period of one year. The request needs to be renewed each year.

7. **Security and Unwanted E-mail**

E-mail users have the responsibility to follow sound security practices, which include the following:

1. E-mail users should not use e-mail services to transfer sensitive data, such as usernames, Social Security numbers, and account numbers over the Internet. Sensitive data passed via e-mail over the Internet could be read by parties other than the intended recipients, particularly if it is clear text traffic. Malicious third parties could potentially intercept and manipulate e-mail traffic. LN staff will send user information only to DOE Lotus Notes accounts.

2. In an effort to combat propagation of e-mail viruses, certain attachment types may be stripped at the DOE network gateway.

3. Attachments can contain viruses and other malware. User should only open attachments from known and trusted correspondents. Infected e-mail can automatically be stopped at the DOE's firewall.

4. Spam is automatically filtered at the corporate gateway in a highly efficient manner. Errors, whereby spam is not filtered can occur. User should delete unsolicited e-mail.

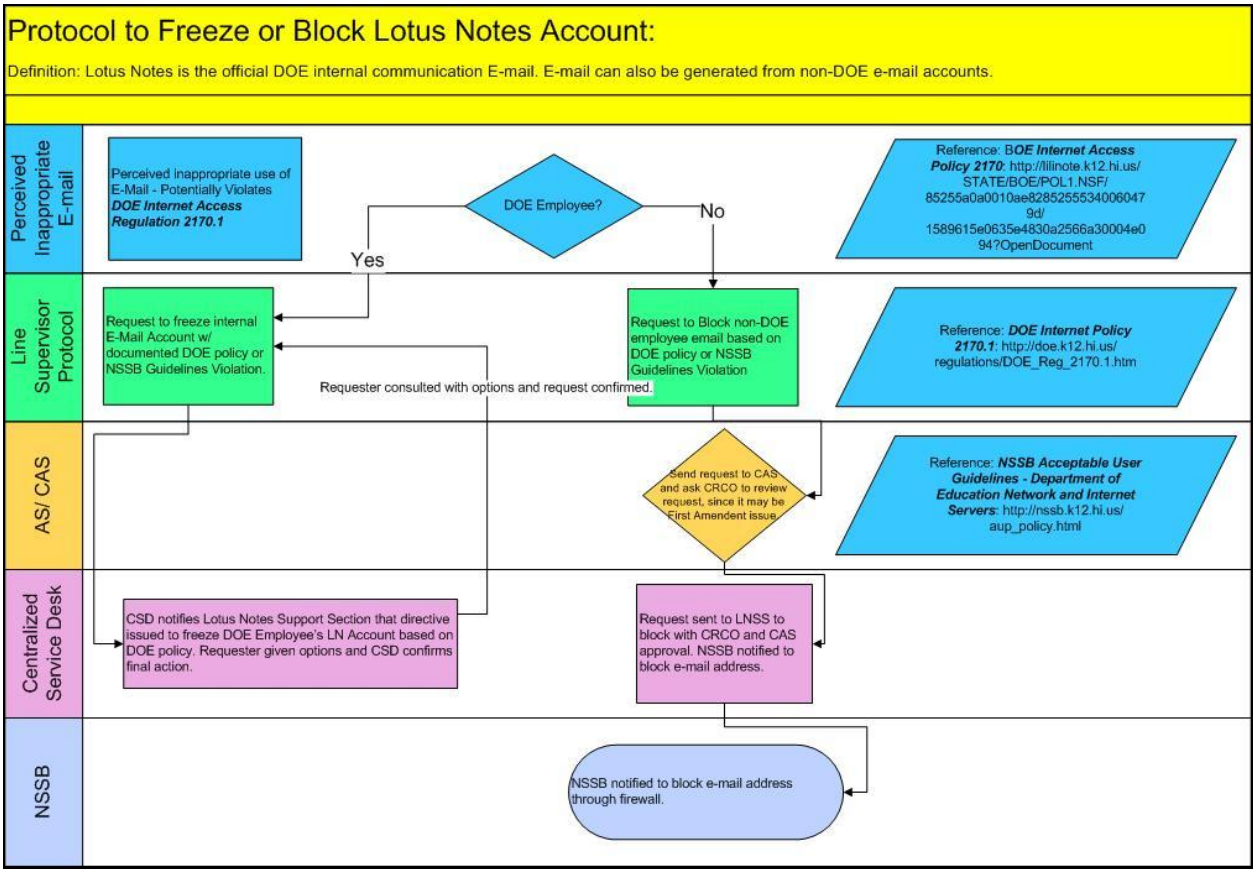
5. Users will not be asked for personal information such as account numbers, Social Security number, home address, or home telephone. Any such requests should be deleted. Such approaches — known as phishing — are fraudulent approaches carried out for purpose of unlawful exploitation.

8. Protocol for Freezing or E-Mail Accounts and Blocking Non-DOE E-Mail

The DOE has practices and procedures in place to protect the integrity and maintain the efficiency of electronic messaging resources, to achieve DOE objectives and meet various regulations. These practices and procedures are subject to change, as appropriate or required under circumstances.

Administrative requests to suspend user privileges. The following written, administrative requests to the Lotus Notes Support Section to provide an audit trail of the request.

A. **Protocol Graphic**



B. **Freezing Accounts and Blocking E-Mail**

1. **Freezing Accounts**

An e-mail is sent to help_notes@notes.k12.hi.us to freeze or suspend an employee's e-mail account by the employee's supervisor or higher level administrator with the rationale for the suspension, which cites DOE policies and guidelines above. The request will be forwarded to the Server Administrator to freeze the user's e-mail account.

2. **Blocking non-DOE Employee's E-mail Address**

E-mail will automatically be blocked by one of several enterprise level anti-virus, spam blocking, anti-phishing, or other malware filters if malware is detected in any e-mail.

Requests to block a non-DOE employee e-mail address will be forwarded to the appropriate Assistant Superintendent and reviewed by the Civil Rights Compliance Office. Approval of the block will be sent from the CRCO to the Lotus Notes Server Administrator to block the user's e-mail address.

9. **Governance and Enforcement**

These guidelines were reviewed representatives from the Office of Information Technology Services (OITS), Network Support Services Branch (NSSB), Office of Human Resources (OHR), and the Civil Rights Compliance Office (CRCO). These offices will review these guidelines annually to assure that HIDOE is in compliance with internal or external requirements. Outside forces that have shaped the terms of these guidelines include laws, such as but not limited to the federal Electronic Communication Privacy Act and the state's Uniform Information Practices Act (Modified). Internally, the DOE Internet Access Policy and Regulations and NSSB's Acceptable User Guidelines were referenced to shape these guidelines.

The DOE and its employees and end users could face legal liability if users violate the terms of the Internet Access policy, regulations, guidelines, and any other related DOE policies or procedures relating to internet and computer use. Therefore, compliance of these policies, regulations, and guidelines will be strictly enforced. If an employee is found through an investigation to have engaged in inappropriate use or conduct resulting from using the DOE's internet or e-mail system, they face progressive disciplinary steps which include the following: informal warnings, written formal warnings, which could result in the loss of e-mail privileges, and other sanctions up to and including termination.

For assistance with the Internet Access Policies, Regulations, and these guidelines, please contact the Lotus Notes Support Section Administrator, Daijo Kaneshiro.

This draft was updated on June 8, 2009.

10. **Acronym Key and Glossary Terms**

AUG	Acceptable User Guidelines - Department of Education Network and Internet Servers
AUP	Acceptable Use Policy
AG	Attorney General
DOE	Department of Education
ECPC	Electronic Communications Privacy Act
GRS	General Records Schedules
HIPAA	Health Insurance Portability and Accountability Act
HRS	Hawaii Revised Statutes
HTTP	Hypertext Transfer Protocol
IAR	Internet Access Regulations - Department of Education
OBS	Offices of Business Services
OIP	Office of Information Practices
OITS	Office of Information Technology Services
NSSB	Network Support Services Branch
OHR	Office of Human Resources
UIPA	Uniform Information Practices Act (Modified)

11. **References, Resources, and Forms**

General Records Schedules 1-11. Form No: 11.7 Electronic Mail Records. Date revised: 02/04/2003. <LILINOTE/ROOTSERVER/HIDOE STATE\OITS\GRS.NSF>.

Hawaii. Office of Information Practices. "Uniform Information Practices (Modified)." Hawaii Revised Statutes. Chapter 92F. 2004 Cumulative Supplement. 10 Jan. 2007 <http://www.hawaii.gov/oip/uipa.html>.

Introduction To that end, the UIPA mandates that all government records be open to public inspection unless access is specifically restricted or closed by law.

92F-3 "Government record" means information maintained by an agency in written, auditory, visual, electronic, or other physical format.

92F-13 For any record that does not fall into a category that must always be disclosed, the UIPA provides that it is a public record unless one of the five exceptions to disclosure under Part II applies. If an exception only applies to a portion of a record, the agency must provide access to the remaining portion of the record.

Hawaii. Board of Education. "2170 Internet Access Policy." Board of Education. State of Hawaii. Department of Education. Oct. 1997. 10 Jan. 2007 <http://lilinote.k12.hi.us/STATE/BOE/POL1.NSF/85255a0a0010ae82852555340060479d/1589615e0635e4830a2566a30004e094?OpenDocument>.

Hawaii. Department of Education. 2170.1 Internet Access Regulations . Aug. 2000 <http://doe.k12.hi.us/regulations/DOE_Reg_2170.1.htm>.

Hawaii. Network Support Services Branch. "Acceptable User Guidelines - Department of Education Network and Internet Servers." NSSB - Network Services Support Branch. 29 Nov. 2004. 10 Jan. 2007 <http://nssb.k12.hi.us/aup_policy.html>.
McAlpine, Fraser A and Droke, Michael. "Electronic Privacy In Employment." FindLaw. 1 Jan. 1998. 10 Jan. 2007 <http://library.findlaw.com/1998/Jan/

SP 3750: Proper Use of Network and Internet Resources; Guidelines for

1. **Purpose**
   To provide guidelines in using the DOE's data, voice, video networking, and Internet resources.

2. **Effective**
   Immediately.

3. **Applies to**
   All employees, students, guests and anyone else authorized to access the DOE's network/Internet and other networked resources. (These individuals are referred to as "users".)

4. **Scope**
   Networking and Internet resources include hardware, software, data system and network, voice system and network, video system and network, Internet, and other networked systems and devices that are owned by the DOE. These resources include

those that enable remote and local communication or access between various computing resources, Local Area Networks (LAN), Wide Area Networks (WAN), voice communications, and video transmission and reception.

5. **Use Policy**

The DOE's networking resources shall be used to support the mission of the Department of Education. These resources shall be used for legal purposes only. They shall not be used for any purpose that is dishonest, disruptive, threatening, or damaging to the reputation of the DOE, inconsistent with the DOE's mission, or likely to subject the DOE to liability.

6. **Authorization and Acceptance**

The Superintendent, the Deputy Superintendent, assistant superintendents, complex area superintendents, principals, and branch directors or their designees shall authorize the use of the network resources. The use of the DOE's network resources requires the user to accept and agree to all the terms and conditions in this standard of practice. Guests and Non-DOE users all require authorization to connect to the DOE network and are subject to all terms and conditions in this standard of practice.

7. **Privacy**

There should be no proprietary interest and no reasonable expectation of privacy while using the network resources provided by the DOE. The DOE may view information and data transmitted, received, processed and stored on DOE resources and may obtain access to the information at any time. The network resources and data provided by the DOE are considered the property of the DOE. These data and/or information may be disclosed to law enforcement or other third parties without prior consent of the user when deemed necessary.

Note: This does not give any DOE representative or any user the right to access, or disclose personal and private information stored in DOE Data Bases without proper authority. Examples: Individual Social Security Numbers, Individual health or medical information, etc.

8. **Network Users' Responsibilities**

A. Become familiar with this SP and other supporting and applicable policies and guidelines contained in the References and Resources Section below.
B. Shall not waste the networking resources or unfairly monopolize resources to the exclusion of others.
C. Act lawfully, ethically, respectfully, and responsibly in the use of resources. Users shall maintain the confidentiality of classified materials, and transmit or disclose classified information only to parties who are authorized to receive or view the classified information.
D. Take all reasonable precautions to protect the DOE's networked resources from unauthorized access and use, by taking prudent and reasonable steps to ensure security.

9. **Prohibited Activities**

DOE prohibits activities that are in violation of any federal, state, or other applicable laws, rules, regulations, and established policies and procedures that include, but are not limited to:

A. Users are prohibited from circumventing the security controls of the DOE resources in trying to access unauthorized resources.
B. Users are prohibited from illegally copying materials that are protected under copyright law or making such materials available to others for copying.
C. Users are prohibited from sending and receiving copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior approval from the authorities.
D. Users are prohibited from installing networking devices and systems that access the DOE network without explicit approval by the department's designated authority.
E. Users are prohibited from using the DOE network resources for any personal or private gain, commercial or profit making activities, and political, religious, or other solicitation.
F. Users shall not conduct unlawful and unethical activities using the DOE resources.
G. Users are prohibited from using the resources to intentionally access, download, display, transmit, or store information that is prohibited by the DOE.
H. Users are prohibited from any actions that may violate the Department's policies using the network resources.
I. Users are prohibited from using profanity or vulgarity and making defamatory comments and actions when using the network resources.
J. Users shall not attempt or engage in or contribute to any activity that may compromise the security of the DOE's network and information technology resources, or to subvert them in any other way.
K. Users are prohibited from removing any component of the DOE network resources without the expressed approval from the Department's designated authority.
L. Users are prohibited from making unauthorized statement's or commitments on behalf of the DOE, or posting any unauthorized web pages.
M. Users are prohibited from altering, destroying, falsifying, or otherwise tampering with official DOE information without proper authorization.

10. **Disclaimer of Liability for Internet Use**

A. DOE filters and prohibits access to certain inappropriate Internet sites that are determined by the Board of Education (Please refer to: http://nssb.k12.hi.us/contentfiltering.html). However, it is difficult to filter all inappropriate and offensive materials. Users may encounter materials that may be offensive and inappropriate.
B. Users access the Internet at their own risk.
C. DOE is not responsible for the materials viewed or downloaded by users from the Internet.
    1) Users shall exercise appropriate judgment when using materials accessed from the Internet.
    2) Users should be aware that having electronic mail addresses on the Internet may lead to receipt of unsolicited e-mail that may have offensive content.

11. **Monitoring and Enforcement**

A. The DOE is the owner or custodian of the network resources, data and information stored on, processed by, or transmitted through the DOE's network resources.

B. The DOE shall at any time, and without prior notice, examine data and information for the purpose such as, but not limited to, ensuring compliance with applicable Department policies, regulations, and rules; monitoring performance of networking resources; and conducting investigations.
C. The DOE has the right to monitor, review, audit and/or disclose any and all aspects of the use of the information and networking resources by the users.
D. The DOE reserves the right, without advanced notice to users, to revoke access to information and network resources.
E. The DOE reserves the right to override the users' passwords without notice or to require users to disclose passwords and/or codes to facilitate access to information processed and stored in the DOE's information resources.
F. Violation of this SP may result in immediate revocation or curtailment of the DOE network resources, in disciplinary action that may include termination, and in civil or criminal liability

12. **Guest and Non-DOE Agencies Access**

A. All guidelines and policies listed in this SP apply to Guest and Non-DOE agencies authorized to connect into the DOE network.
B. Guests and Non-DOE agencies are responsible for installing anti-virus, anti-malware, anti-spyware software on their computers and keeping them up-to-date at their own cost. Also the computer operating system and applications need to be kept up-to-date with the latest security patches and upgrades.
C. If the Guest or Non-DOE computers are found to be in non-compliance, they will be immediately removed from the DOE's network. If the spread of viruses/worms, malware, trojans and other software vermin is caused by a Guest or Non-DOE computer that has not been kept up-to-date per paragraph B above and it is determined to be negligent then all remediation costs will be charged to the Guest or Non-DOE agency.

13. **SP Maintenance Responsibility**

The Telecom Director in the Office of Information Technology Services is responsible for maintenance and questions regarding this SP document.

The Frequently Asked Questions (FAQ) page for this SP provides standard responses to common questions. Please review this resource before inquiring via telephone. **See Reference (a) below.**

14. **References and Resources**

The following resources may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.

(a) Frequently Asked Questions (FAQ) for SP 3750
(b) BOE Policy 2170 Policy
(c) Internet Access Regulation
(d) NSSB Acceptable Use Guideline
(e) NSSB Makani E-Mail Policy

SP 3760: Guidelines for Wireless Access Network Installation & Operations

1. **Purpose**
   To describe how wireless technologies are to be deployed, administered, and supported within the DOE network.

2. **Effective**
   Immediately.

3. **Applies to**
   All DOE wireless computer users. These include authorized Guests and Non-DOE agencies connecting into the DOE network via wireless devices.

4. **Action Required**

   A. **Wireless Access Guidelines and Procedures**

   The Wireless Access Guidelines and Procedures are established to ensure secure and reliable access to limited network resources for all members of the DOE community for educational purposes. The DOE network infrastructure can be extended through the use of wireless network access methods. This SP describes how wireless technologies are to be deployed and operated as to protect the security and integrity of the entire DOE network. Use of the DOE network (wired and wireless) is governed by Board of Education (BOE) Internet **Access Regulations 2170.1**, SP 3750 Proper Use of Network and Internet Resources, and this standard of practice which is an extension of the **Regulation 2170.1.**

   Network Support Services Branch (NSSB) of the Office of Information and Technology Services (OITS) is responsible for ensuring the integrity, reliability, and security of the DOE network infrastructure. NSSB can:

   1) Restrict the use of wireless devices.

   2) Determine what wireless devices can be connected to the network.

   3) Determine how these devices should be configured.

   B. **Overview**
   Wireless devices offer increased flexibility, expandability, and mobility; thus improving access to networked resources. Unsecured and improperly implemented wireless devices pose risks to the network. When wireless implementations are done without proper security and little or no planning, they can impact the security and productivity of many users on the network.

   These Guidelines and Procedures:

1) Provides for an acceptable level of wireless security.

2) Provides for network robustness/reliability.

3) Minimizes network interference from other devices utilizing the same wireless frequency spectrum.

C. **Scope**

This SP applies to all devices using wireless communications (e.g. computers, PDAs, voice over IP phones, printers/scanners) that interface directly with the DOE network. This includes but is not limited to: wireless access points, wireless routers, wireless base stations, and any wireless communication device capable of transmitting and receiving data packets on the DOE network. Wireless devices such as personal cell phones that do not interface with the DOE's network do not fall under the scope of this standard of practice.

D. **Specific Procedures to Comply with Wireless Access**

1) Register the Wireless Access Points (AP), Base Stations (BS) and devices in a centralized database. Go to http://wificentral.k12.hi.us/wifi to register the wireless devices. If you do not know your login or password, send an email to nssb@k12.hi.us for assistance.

   a. The school or office administration (Principal/Administrator) authorizes implementation of the wireless device and ensures that the wireless device is registered in the central database of authorized wireless devices connected to the DOE network, including the school local area networks (LAN). This centralized database, at a minimum, must contain the basic information of the wireless device including the manufacturer, model number, location of placement, IP address assigned, name of the AP/BS, MAC address, frequencies used, channel used, security configuration (Encryption, Authentication, etc), and point of contact responsible for the wireless device.

   b. All implemented wireless devices are subject to audits. The audits will check for proper implementation and security safeguards. Also traffic transmitted over the wireless network is subject to monitoring.

2) **Suitability**

   a. For data networks, wireless networks should be considered an extension, not a replacement for an existing wired network. At some point, wireless networks need to connect into a wired network.

   b. Wireless access should only be allowed with the latest encrypted protocols and/or Virtual Private Network (VPN) when accessing administrative information systems such as the Financial Management System (FMS), Student Information System, and Human Resource Systems that contain sensitive and confidential information.

c. DOE reserves the right to restrict wireless access that is disruptive to the network, or that poses a threat to the DOE's information security and resources.

d. DOE has the right to perform audits or accreditation of the wireless network.

3) **Management and Support**

a. Wireless LAN implementations are the responsibility of the Administrator
(E.g. Complex Area Superintendent, Principal for school, office administrator for state or complex office), who controls and is responsible for the operational space, such as boundaries of school campuses or office work space areas. The Administration is expected to know what is occurring in the operational space; and to take steps to make sure that all wireless implementations active in their space follow the standards of practice defined here.

b. Authorized by Administration. Every wireless access installation within the DOE network must be authorized by the Administrator in which it operates. Administration may delegate details to technical staff or other responsible person. Network access using an unauthorized and unregistered wireless device (considered a rogue device) is prohibited and is subject to confiscation.

4) **Radio Frequency Spectrum Management**

a. There are many devices that share the same radio frequency spectrum as most of the DOE Wireless Network. This includes, but is not limited to 2.4 GHz and 5 GHz devices such as cordless phones, microwave ovens, wireless cameras or speakers that can interfere with the wireless network. To prevent such disruptions of the wireless networks, a site survey should be conducted to identify trouble spots and to optimize the placement of wireless devices.

b. Wireless channel assignments will be managed by the School's Administration.

5) **Security Standards**

a. Wireless Access Points (AP)/Base Stations (BS) should be configured as a closed network. Every effort shall be made to limit the signal range of the wireless access to the school campus or office space under the jurisdiction of the Administrator. Wireless access is not allowed from the outside perimeters of the school or office premises.

b. Wireless infrastructure, by nature, is insecure because data is transmitted via air using radio waves that anyone can intercept and capture. It is recommended that wireless transmissions be encrypted with the latest protocols/technologies especially if accessing sensitive student or financial data.

c. All authorized wireless users or clients shall be known to the

AP/BS. Wireless user access shall require authentication, authorization, and proper accounting of the access.

d. Wireless access Service Set Identifier (SSID) should be changed from the vendor's default settings, and SSID beaconing should be disabled.

e. Practice limiting off-hour wireless access by turning off AP/BS during non-use hours if possible.

f. Rogue wireless devices (unregistered, unauthorized and unknown to management) are strictly prohibited. Rogue wireless devices will removed and confiscated if discovered on the DOE network. Repeated offenses by an individual can result in locked out access to the network and disciplinary actions by the Administration.

6) **Guest Access (e.g. vendors, parents, community members)**

a. Guests who wish to connect wireless devices onto the DOE network must first obtain permission from the Administration.

b. Administration's Responsibilities:

(1) Guests must be informed that they will only have limited access to the DOE network,

(2) Guest access devices must be clean and verified for acceptable client security (i.e. no viruses, spy ware, malware, infestations of the guest device) before being allowed access to the DOE network, and

(3) Any problem or disruption caused by guest device will be the responsibility of the permitting Administration for remediation.

7) **Enforcement**

Any DOE employee found to have willfully violated this SP shall be subject to disciplinary action as prescribed in the Internet **Access Regulation 2170.1** and as appropriately determined by the Administrator.

5. **SP Maintenance Responsibility**

The Network Support Services Branch (NSSB) of the Office of Information Technology Services (OITS) is responsible for the maintenance, administration, and questions regarding this SP. To request assistance or to suggest improvements, send email to nssb@k12.hi.us.

6. **References, Resources, and Forms**

(a) Institute of Electrical and Electronics Engineers (IEEE) 802.11 Standards. The IEEE 802.11 Standards is a set of standards for implementing wireless local area networks

(b) BOE Regulation 2170.1 - Internet Access Regulation

(c) Standards of Practice (SP) 3750 - Proper Use of Network and Internet Resources

SP 3765: Servers and Network Operating Systems—Security Measures

1. **Purpose**
   To describe standard security measures and appropriate hardware configurations for Servers and Network Operating Systems used in the DOE's schools and offices.

2. **Effective**
   Immediately.

3. **Applies to**
   All personnel and non-DOE personnel responsible for installing and/or managing network servers within the DOE's network or routinely used by personnel for DOE business.

4. **Definition of a Server**
   A server is a network device that provides a service to network users by managing shared resources.

5. **Conditions Requiring Security Measures**
   A. Servers that provide shared services and resources that are critical to school or DOE operations, and/or
   B. Servers that contain confidential DOE data.

6. **Prerequisites for Purchasing Network Servers**
   A. Schools and offices must have a clear purpose for purchasing a server consistent with the Department's mission of student achievement and the DOE's Acceptable Use Policy.
   B. Schools should designate an employee or position that will be responsible for the ongoing management of the server. Hereafter, this designee will be called the "Server Manager," in this document.

      The Server Manager should size and configure network devices used as servers appropriately according to the utilization demands on the shared resources and the impact that temporary loss of these resources would have on daily operations.

7. **Server Hardware Configurations**
   A. All servers containing mission critical applications and/or student data must have a properly sized and configured Uninterruptible Power Supply.
   B. All servers containing mission critical applications and/or student data must have redundant data storage i.e. RAID (Redundant Array of Independent Disks) I, RAID V or scheduled data backups.

8. **Support for Servers and Network Operating Systems**
   The Server Manager can contact NSSB for assistance in the following circumstances.
   A. Preparing appropriate configurations and quotations according to school requirements.
   B. Initial Server installation and configuration**.**

C. Limited application installation and configuration.
D. Ongoing consultation and after-installation support.

See services available on http://nssb.k12.hi.us/noss services.html.

9. **Server Security**
A. All accounts with administrative rights must be password protected.
B. Servers should be kept up-to-date with all critical security patches.
C. All servers and connecting clients must have up-to-date virus protection.
D. Access to confidential data must be restricted to appropriate users.
E. Servers should be physically located in secure areas.

10. **SP Maintenance Responsibility**
The Telecom Director in the Office of Information Technology Services is responsible for maintenance and questions regarding this SP document.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See **Reference (a) below.**

11. **References and Resources**
The following resource may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.
(a) Frequently Asked Questions **(FAQ)** for SP 3765
(b) BOE Policy2170, Internet Access
http://doe.k12.hi.us/technology/internetaccess.htm
(c) NSSB' Web site

SP 3770: Creating Secure User Passwords

1. **Purpose**
To provide general guidelines and best practices in creating user passwords for the DOE's Computer/Networking Systems.

2. **Effective**
Immediately.

3. **Applies to**
All DOE computer users.

4. **Creating Secure Passwords**
A. General Rules for Creating Passwords
When passwords are required there may be different rules that apply for each application or system. Generally passwords are:

1) **Case Sensitive** - Upper-case letter (e. g., A) is not the same as the lower-case letter (e.g., a)
2) **No Spaces Allowed** - Most applications do not allow blank spaces in the password.

3) **Special Characters** - Characters such as a tilde (~) or period (.) may or may not be allowed in the password. It depends on the application or system that the password accesses. For example on a Unix-based system most special characters are allowed in a password, while on a Windows-based system only selected special characters are allowed.
4) **Length** - Most applications have a minimum and maximum length for the password, although you may be allowed to create a password that is only four characters long, for security reasons it is recommended that the minimum length be seven characters.

B. Creating Passwords That Won't Be Easily Cracked

General guidelines to create a password, it should:

1) Be at least seven characters long,
2) Mix letters, numerals and allowed special characters (i.e. dash (-) or underscore (_)),
3) Use upper-case and lower-case letters, and
4) Not contain any words that are in a dictionary for any language. Password crackers will use words in multiple language dictionaries i.e. Hawaiian, Japanese, German, English, etc. in attempting to crack the password.

C. Use Hard-to-Crack Passwords Made Easy-to-Remember

1) Make passwords like the vanity plates on cars. For example: Passwords REZ (passwords are easy)
2) Create a pattern when you create your passwords such as using upper-case letters for vowels and lower-case for consonants, so it would be easy to remember but hard to crack. The word "lokahi" would then be "lOkAhI."
3) Substitute letters for numbers. For example 1=I, 5=S, 0=O, 4=A. Some people do not recommend creating these patterns but if it makes it easy for you to remember, use it. Remember though, that if you use a pattern and then someone finds out your password, you should then change your pattern for your new password.
4) Use a phrase instead of a single word to make it a more secure password, such as "*kokua* for you" would be "Kokua4U" or “Jack & Jill went up the hill” would be “J&Jwuth.”

D. Keeping Your Passwords Secure

1) NEVER give out your passwords to anyone unless you absolutely trust them. The only time you may need to reveal your password to someone (i.e. a trusted system administrator) is when you initially create a password on the system, for troubleshooting, or when you want to change it.
2) Do not write down your password on a slip of paper easily accessible and close to your computer. You may write down your password but keep it in a safe/secure place and don’t associate it with the login name. If you think someone might know your password, have your password changed.

3) Change your passwords periodically. The DOE recommends every six months. Keep it in a safe/secure place and don't associate it with the login name. If someone is sitting near you when you have to enter a password, be sure to cover the keyboard or block their view while typing in your password.

5. **SP Maintenance Responsibility**

The Office of Network Support Services Branch (NSSB) of the Office of Information Technology Services (OITS) is responsible for the maintenance, administration, and questions regarding this SP.

The Frequently Asked Questions (FAQ) page for this SP may provide standard responses to common questions. Please review this resource before inquiring via telephone. See **Reference (a) below.**

6. **References, Resources, and Forms**

The following resource may provide access to statutory, policy, and contractual authorities; and closely related SPs, procedures, and forms.

(a) Frequently Asked Questions (FAQ) for SP 3770