



North Carolina Department of
Information Technology

Employee Manual

May 2017

CONTENTS

INTRODUCTION	1
STATEWIDE POLICIES ADOPTED BY REFERENCE, ADDITIONAL AUTHORITY	1
SCOPE	1
DIT POLICY AUTHORITY AND OWNERSHIP	1
REVISION HISTORY	1
USER NOTE	1
SECTION 1 HUMAN RESOURCES.....	2
STATE HUMAN RESOURCES POLICIES	2
DIT HUMAN RESOURCES POLICIES	2
<i>Employment and Records</i>	2
1.1 Background Investigations of DIT Personnel and Contractors.....	2
1.2 Employee and Contractor Annual Training	3
1.3 New Employee Orientation	4
1.4 Open-Door Policy.....	4
1.5 Privacy For Use of IT Resources	4
1.6 Onboarding and Termination of DIT Employees and Contractors	5
1.7 Issuance of Mobile Communication Devices	5
1.8 Allowance for Use of Personal Mobile Telephones and Mobile Communication Devices	6
1.9 Parking	6
1.10 Emergency or Disaster Situations Expense Reimbursement	7
1.11 Payment of Membership Dues	8
1.12 Teleworking	8
1.13 Employee Responsibilities under the DIT Policy Manual.....	11
1.14 Loss, Theft and Misuse of State Property	11
1.15 Separation from Employment and Exit Interview.....	11
1.16 Reduction in Force.....	12
SECTION 2 SECURITY	14
SITE SECURITY	14
2.1 Facility Access	14
2.2 Facility Access After a Change in Job Duties	18
2.3 Semi-Annual Badge Access Certification	18
2.4 Obtaining a Badge Access Report	19
INFORMATION SECURITY	19
2.5 General Information Security	19
2.6 Acceptable Use	19
2.7 Non-DIT Managed End User Devices Policy with Terms and Conditions	21
SECTION 3 WORKPLACE, HEALTH AND SAFETY POLICIES	23
3.1 Use of State Property and Facilities.....	23
3.2 Tornado and Severe Weather Warnings	23
3.3 Fire Safety and Evacuation	24
3.4 Bomb Threats	24
3.5 Social Distancing Policy.....	24
SECTION 4 ETHICS	25
4.1 Ethical Standards: Vendor Gifts and Gratuities	25
4.2 Misuse of Position.....	26
4.3 Secondary Employment.....	26
4.4 Disclosure Statements and Mandatory Training	26
SECTION 5 PUBLIC RECORDS	27

5.1 Public Requests for DIT Records.....	27
5.2 Public Requests for DIT Customer Records.....	27
5.3 Access to Procurement File Records.....	27
SECTION 6 PROCUREMENT	28
6.1 Procurement.....	28
SECTION 7 LEGISLATIVE AND MEDIA CONTACTS	28
7.1 Legislative Contacts	28
7.2 Media Contacts.....	29
SECTION 8 INTERNAL AUDIT	29
8.1 Internal Audit Responsibilities.....	29
SECTION 9 ACCESS TO LEGAL COUNSEL.....	30
9.1 Access to Legal Counsel.....	30
SECTION 10 DIT WEBSITE USAGE AND ACCESSIBILITY	31
10.1 DIT Website Usage.....	31
10.2 Website Accessibility	31
SECTION 11 RECORDS RETENTION	32
11.1 Records Retention	32
SECTION 12 BUDGET AND FISCAL POLICIES	33
BUDGET POLICIES	33
12.1 Budget Development and Execution	33
FISCAL POLICIES	33
12.2 Statewide Fiscal Policies Apply	33
<i>Office of State Controller Fiscal Policies.....</i>	<i>33</i>
<i>OSBM Fiscal Policies</i>	<i>34</i>
SECTION 13 POLICY MANUAL REVIEW AND UPDATES.....	34
13.1 Policy and Procedures Review and Revision Process.....	34
APPENDIX A: ETHICS GUIDELINES	35

INTRODUCTION

STATEWIDE POLICIES ADOPTED BY REFERENCE, ADDITIONAL AUTHORITY

As an agency of the State of North Carolina, the Department of Information Technology (DIT) is governed by state law and statewide policies, which are incorporated by reference. Those include, but are not limited to:

- The [State Human Resources Manual](#) (OSHR Manual)
Note: Not all DIT employees are covered by the [N.C. Human Resources Act](#). The State CIO and Deputy State CIOs are exempt under [G.S. 143B-1322\(b\)](#). Other managerial and policy making positions may be exempt under the same statute.

Employees of the Health Information Exchange Authority are exempt from some portions of the act under [G.S. 126-5\(c11\)\(32\)](#).

Some DIT employees are voluntarily exempt from portions of the act under [G.S. 126-5\(c11\)\(3\)](#).

New positions created after the formation of DIT are exempt from the act under [G.S. 143B-1336\(e\)](#).

ADDITIONAL AUTHORITY:

- The N.C. [Public Records](#) act and the [Public Records and Archives](#) statute
- The [State Budget Manual](#)
- [EAGLE](#) and other [policies](#) administered by the Office of State Controller
- The [Statewide Information Security Manual](#)
- [North Carolina IT Procurement Policies and Procedures](#)
- [North Carolina Procurement Rules](#)

SCOPE

The policies and procedures in this manual apply to all DIT employees, and to contractors where specified.

DIT POLICY AUTHORITY AND OWNERSHIP

All DIT policies are adopted pursuant to the State CIO's statutory authority under [Article 15 of G.S. 143B](#) and other statutes.

The DIT Policies and Procedures group is responsible for maintaining the DIT Employee Manual, helping develop clear and concise policies, and ensuring they are easily accessible to DIT employees. The group also coordinates the annual review of the manual with DIT divisions.

REVISION HISTORY

This policy manual is effective May XX, 2017, and supersedes the Office of Information Technology Policy Manual dates July 2016.

USER NOTE

Blue, underlined text contains a hyperlink to the relevant document or section.

SECTION 1 HUMAN RESOURCES

STATE HUMAN RESOURCES POLICIES

[Classification](#)
[Discipline, Appeals and Grievance](#)
[Equal Employment Opportunity](#)
[Employee Benefits and Rewards](#)
[Employment and Records](#)
[Leave](#)
[Performance Management](#)
[Recruitment, Selection and Workforce Planning](#)
[Safety](#)
[Salary Administration](#)
[Separation](#)
[State HR System](#)
[Statutory Provisions](#)
[Training](#)
[Wellness and Work-Life Balance](#)
[Workers' Compensation](#)

DIT HUMAN RESOURCES POLICIES

EMPLOYMENT AND RECORDS

1.1 BACKGROUND INVESTIGATIONS OF DIT PERSONNEL AND CONTRACTORS

Purpose

To require background investigations and other security measures for DIT personnel and contractors.

Owner

Human Resources

Policy

Contractors and applicants for employment at DIT must undergo a background investigation, including a criminal history record check, pursuant to [G.S. 143B-1336\(g\)](#). Criminal background investigations are also required for those participating in the Interchange of Government Employees program described in [Article 10 of G.S. 126-51](#).

Applicants who have completed a state job application and are interviewed for a position or promotion at DIT will be requested to sign a Criminal Background Investigation Authorization Form. Refusal to provide adequate or correct information on this form or to provide consent for the investigation will result in withdrawal of the applicant from consideration for the position.

Pending the completion of the SBI criminal history record check for those individuals who require one, DIT will perform preliminary criminal background investigations on employees and contractors.

The existence of a felony conviction or of a misdemeanor conviction which involves fraud, false statement or deception will not automatically disqualify the applicant from employment. DIT will inquire further into the matter and make a determination entirely within its discretion to accept or reject the applicant considering such things as

the date, nature and number of convictions, the relationship the convictions bear to the duties and responsibilities of the position, and other pertinent facts.

Individuals who are DIT employees who have not had a criminal background investigation performed because they were hired before passage of [G.S. 143B-1336\(g\)](#) will be requested to sign a Criminal Background Investigation Authorization Form. If a background investigation reveals the existence of a felony conviction or a misdemeanor conviction which involves fraud, false statement or deception, DIT will inquire further into the matter and consider reassigning the individual, consistent with state law and Office of State Human Resource policies. In making a determination, DIT will consider the date, nature and number of convictions, the relationship the convictions bear to the duties and responsibilities of the position, and other pertinent facts.

1.2 EMPLOYEE AND CONTRACTOR ANNUAL TRAINING

Purpose

To establish policies governing mandatory annual employee and contractor training.

Owner

Human Resources
Enterprise Risk and Security

Policy

All DIT employees and contractors are required to complete annual training on a schedule and topics determined by Human Resources and Enterprise Risk and Security.

DIT employees may be required to sign and date forms prepared by Human Resources and Enterprise Risk and Security acknowledging that they have completed required training.

Annual training topics may include, but are not limited to, the following:

- FEMA Continuity Planning
- Continuity Management
- Facility Safety
- Identity Management
- Immediate Response to a Critical Incident
- Information Security Training
- Phishing
- Policies, Privacy and Public Records
- Records Retention
- Statewide Information Security
- IRS Disclosure Awareness Training

Specific training topics for a given year will be included in the annual training announcement sent to all DIT employees.

Key Personnel Annual Training

Key personnel are defined as system administrators and information security officers. Due to the specialized nature of these positions and their critical role in providing IT security, additional annual training shall be provided to employees in these positions. The Chief Information Risk/Security Officer will determine the employees or job classifications to receive additional training.

1.3 NEW EMPLOYEE ORIENTATION

Purpose

To require an orientation session for all new DIT employees and contractors to answer any questions an employee has and to provide information about DIT, work hours, policies, procedures, benefits and any other topics deemed appropriate by Human Resources.

Owner

Human Resources

Policy

New employees must attend an individual orientation session and a department-wide orientation.

DIT Human Resources will schedule the individual orientation within three working days after hire. The department-wide orientation will be held monthly.

Exceptions to this policy may be approved by the DIT Human Resources Director on a case-by-case basis.

1.4 OPEN-DOOR POLICY

Purpose

To establish a policy for employee access to the State CIO.

Owner

State CIO

Policy

The State CIO has an open door policy for DIT employees. Any employee can request a meeting by submitting an email to the State CIO's executive assistant.

1.5 PRIVACY FOR USE OF IT RESOURCES

Purpose

To notify DIT employees and contractors that their use of IT resources may be monitored, and they have no expectation of privacy.

Owner

Human Resources
Enterprise Risk and Security Services

Policy

Use of information technology resources in DIT is not private.

Information concerning online data processing activities is routinely captured as part of normal business operations. This information is stored in items such as system logs, backup tapes, and disks, and is subject to internal and external audits. Deleting an electronic record does not assure that it is removed from circulation, as the deleted record may still be retrievable and/or is stored elsewhere.

DIT will report any suspected illegal activities to the appropriate authorities and may take disciplinary action against employees found in violation of state law or policies.

DIT employees and contractors will be notified at orientation that their use of IT resources may be monitored.

Where technically practicable, each computer system must prominently display a warning banner to notify users that their usage is subject to monitoring and stating the terms a user must affirmatively accept before accessing the system.

1.6 ONBOARDING AND TERMINATION OF DIT EMPLOYEES AND CONTRACTORS

Purpose

To establish a policy providing facility access and assets to DIT employees and contractors when they initially report for duty, and revoking access and recovering assets when they leave DIT employment.

Owner

Human Resources

Policy

DIT will establish and revise as needed a documented process for onboarding and terminating employees and contractors. The process must include, but is not limited to, the issuance and return of state assets including personal computers, telephones and mobile communications devices, and access to DIT facilities and data.

DIT Human Resources, in conjunction with DIT organizational units, will develop the process and forms for onboarding and terminating DIT employees and contractors.

The forms will be made available on the DIT Intranet.

1.7 ISSUANCE OF MOBILE COMMUNICATION DEVICES

Purpose

To establish the policy for the issuance of state-owned cellular phones and mobile communication devices to DIT employees.

Owner

Human Resources

Policy

DIT may issue State-owned cellular telephones or mobile devices for state purposes use under guidelines developed by the Cellular Equipment Coordinator and approved by the State CIO.

DIT and employees must comply with policy 5.11 of the [State Budget Manual](#) in the issuance of state-owned devices.

State-issued devices are considered state property and must be used in accordance with all applicable state laws and policies.

In lieu of issuing a state-owned device mobile communication device, DIT may provide an allowance to employees for the business use of personal devices.

1.8 ALLOWANCE FOR USE OF PERSONAL MOBILE TELEPHONES AND MOBILE COMMUNICATION DEVICES

Purpose

To establish the requirements for DIT employees to receive an allowance for use of a personal mobile communication device (MCD) in lieu of a state-issued device.

Owner

Finance

Policy

A DIT employee qualified to receive a state-issued MCD is eligible for an allowance to partially reimburse the employee for the monthly operating costs of a personal MCD, if approved by the employee's Division Director.

The allowance is not intended to cover 100% of the fees and service charges incurred under an individual's monthly service plan. Reimbursement will not be provided for any portion of equipment costs or replacement costs for any loss, theft or damage to the employee's personal mobile communication device or accessories.

DIT will adhere to Policy 5.11 in the [State Budget Manual](#) in providing an allowance in lieu of issuing a state-owned mobile communication device.

Use of all personal devices by employees who receive an allowance must comply with all applicable state laws and security and other policies. Employees are specifically reminded that use of a personal device for state business purposes creates state records subject to N.C. Public Records act ([G.S. 132](#)).

Reimbursement rates will be established by DIT Financial Services and approved by the Office of State Budget and Management. Employees are eligible for reimbursement for two levels of plans: voice only or voice and data plans.

Employees are not eligible for reimbursement for data only plans.

To receive reimbursement, employees must maintain their mobile device plan and must be accessible during regularly scheduled work hours.

Employees who wish to receive an allowance for use of their personal mobile communication device must complete the Personal Mobile Telephone/Mobile Communication Device (MCD) Authorization form, which is available on the DIT Intranet.

1.9 PARKING

Purpose

To establish policies and procedures for employee parking.

Owner

Human Resources

Policy

It is the intent of DIT to ensure that all employees have access to parking within walking distance of their assigned workplace.

Parking at 3700 and 3900 Wake Forest Road, Raleigh

Parking lots are adjacent to both buildings with no assigned parking spaces and no monthly employee fees.

Parking at the Western Data Center

A parking lot is adjacent to the building with no assigned parking spaces and no monthly employee fees.

Parking in Downtown Raleigh

DIT employees who are assigned to a building in downtown Raleigh are assigned a parking space in a State-owned parking lot or deck. See also the following resources:

- [Policies and Procedures for Downtown Raleigh Parking](#)
- [Downtown Raleigh Parking Resources](#)

Procedures

Parking is assigned as part of the new employee on-boarding process. The employee’s manager should notify the DIT Parking Coordinator if a parking space in downtown Raleigh is required.

Employees may park in any space in the lots adjacent to DIT buildings.

Requirements

- Employees shall observe safe speeds and obey all directional signs erected in the parking lots.
- In the event of an accident in a State-owned parking lot, the involved parties shall notify State Capitol Police.
- Damage to vehicles caused by reasons other than collision with another vehicle should be reported to DIT HR.

1.10 EMERGENCY OR DISASTER SITUATIONS EXPENSE REIMBURSEMENT

Purpose

To establish policies and procedures to reimburse DIT employees for out-of-pocket expenses for meals and lodging during emergency or disaster situations.

Owner

Finance

Policy

DIT employees may be reimbursed for out-of-pocket expenses for meals and lodging during an emergency or disaster situation that endangers DIT facilities or severely disrupts DIT services. Examples of emergency or disaster situations are severe weather, such as hurricanes or ice storms, cyberattacks, and catastrophic failures.

The State CIO must designate an event as an emergency or disaster situation for employees to be eligible for reimbursement.

Requirements

Only employees working at their regular duty station are eligible for reimbursement. Employees previously approved for overnight travel during the emergency or disaster situation are not eligible for reimbursement.

Meals

Employees who work for 12 or more hours during an emergency or disaster situation are eligible for meal reimbursement. The maximum amount for reimbursement is \$10.00 for each 12-hour period of continuous work.

For example:

Time Worked	Reimbursement Amount
Less than 12 hours	\$0

12 hours – less than 24 hours	\$10.00 maximum
24 hours – less than 36 hours	\$20.00 maximum

Receiving snacks during emergencies or disaster situations does not preclude employees from also receiving meal reimbursement. The meal reimbursement is meant to provide some compensation for meals, not snacks.

Lodging

If possible, overnight lodging is arranged for employees in advance and payment is made directly by DIT. For lodging costs not otherwise covered by DIT, reimbursement is available for employees who are:

- 1) Required to work during the emergency or disaster situation; and
- 2) Are unable to safely return home at night; or are asked to remain close to the worksite in anticipation of emergency or disaster conditions.

An employee must complete the Emergency Expense Reimbursement form, which must be approved by the employee’s supervisor, to receive reimbursement.

1.11 PAYMENT OF MEMBERSHIP DUES

Purpose

To establish a policy for the payment of membership dues for DIT employees to associations, clubs and organizations.

Owner

Finance

Policy

DIT will pay membership dues for DIT employees only where the membership benefits the state.

Memberships may be in the name of an individual; however, DIT’s payment shall terminate at the same time that the individual’s employment with the state terminates.

1.12 TELEWORKING

Purpose

To establish a policy allowing DIT employees to telework.

Owner

Human Resources

Definitions

Official duty station: An employee's official place of work. Typically, a duty station is a state facility. An employee's home may be the official duty station if approved by the employee’s manager and the employee’s division director.

Alternate work location: a work site other than a central workplace, such as an employee’s home or satellite state office. An alternate work location does not include a location where an employee works for limited periods of time or infrequently.

Policy

DIT employees may telework, either full- or part-time, subject to policies established by the Office of State Human Resources and DIT.

Approval for telework or use of an alternate work location does not change an employee's official duty station.

The decision to allow a DIT employee to telework is wholly in management's discretion and may not be appealed.

DIT may terminate the teleworking agreement at its discretion. Termination of a teleworking arrangement by management may not be appealed.

Teleworking assignments do not change the conditions of employment or required compliance with policies and rules. All teleworking arrangements shall be documented with a written description of the responsibilities of both DIT and the employee. Each participant in a teleworking arrangement must sign the document that contains the terms of the teleworking arrangement. Periodic reviews of adherence to the telework policies may be conducted by DIT management. The document shall define the parameters of the teleworking arrangement and shall comply with the following policy provisions.

An official duty station not located in a state facility, such as an employee's home, does not change the conditions of employment or required compliance with policies and rules.

Compensation and Benefits

An employee's compensation and benefits will not change due to teleworking.

Travel Reimbursement

Pursuant to the State Budget Manual, travel reimbursement for all employees is computed from the employee's official duty station. Section 5.1.26 of the [State Budget Manual](#) states that reimbursement for travel is based on "the closer of duty station or point of departure to destination."

Safety and Liability

The supervisor shall provide reasonable assurance that materials, equipment and furniture supplied by DIT to the employee at the alternate work location comply with safety standards.

Restricted-Access Materials

DIT supervisors must grant permission for teleworkers to work on restricted-access information or materials at alternate work locations. Teleworkers shall agree to follow agency-approved security procedures in order to ensure confidentiality, availability, and security of data.

Work Hours

The total number of hours that employees are expected to work will not change, whether at the office or at the alternate work location. This does not, however, restrict the use of alternative work schedules. DIT will track the work hours of employees who telework and document the hours worked by employees covered by the Fair Labor Standards Act. Employees shall apply themselves to their work during designated work hours and not engage in activities that are not work-related.

Equipment and Software

DIT shall establish the conditions by which the state will pay for phone and other services furnished to teleworkers.

Work Assignments

An employee's work assignment will not change or be different from a non-teleworker's assignments with the same job description, except as necessary in the normal course of business.

The policies and procedures that normally apply to the central workplace shall remain the same for teleworking employees. These include:

- Performance management
- All safety requirements
- Data security requirements.

The State CIO may waive all requirements described in this policy pursuant to the Office of State Human Resources [Communicable Disease Emergency Policy](#).

Requirements

A supervisor may request permission to allow an employee to telework when the following criteria are met.

The position has tasks that are portable and can be performed away from the main worksite. Such tasks include:

- data analysis
- remote administration of assets or systems
- serving customer accounts
- reviewing documents/contracts
- writing decisions/reports
- setting up conferences
- data entry
- word processing
- phone intensive tasks.

The employee has a performance rating of at least “Meets Expectations,” as defined in the Office of State Human Resources [Performance Management Policy](#), in the previous and current year performance reviews. This requirement may be waived if the employee has not received a performance review while employed at DIT.

The employee does not need close supervision and has few mandated interactions with co-workers and/or the public at an assigned duty station. If public contact is required, the supervisor shall outline how the employee can meet the requirements for necessary face-to-face contact or other types of main office contact required by the job.

The employee possesses a high level of skill and knowledge of the job.

The employee is computer literate and has a designated and secure area at the alternative work location for the completion of work assignments.

The employee’s work can be monitored with quantifiable tasks, and quantity and quality can be measured. For non-quantifiable or project oriented tasks, measuring normally involves: establishing the nature and objectives of the tasks; setting a deadline or due date; and, setting progress or status report meetings.

A supervisor must demonstrate that the above criteria are met by submitting a request to the DIT Human Resources Office that identifies the individual proposed for teleworking and a detailed description of the employee’s telework arrangement.

If the Human Resources Director approves the arrangement, the request will be submitted to the employee’s division manager for approval. If the request is rejected, the reason for rejection must be documented on the request and returned to the supervisor.

Employees may not request permission to telework directly to the Human Resources Office.

1.13 EMPLOYEE RESPONSIBILITIES UNDER THE DIT POLICY MANUAL

Purpose

To provide a policy regarding employees' awareness of their responsibility for understanding the contents of the DIT Policy Manual and its ongoing update process, including a formal acknowledgement of the responsibility.

Owner

Human Resources

Policy

All employees are responsible for understanding the contents of the DIT Policy Manual, complying with its applicable provisions and signing a statement acknowledging their responsibilities.

Employees have a continuing responsibility to be aware of any changes to this DIT Employee Manual. Employees will be notified promptly of any significant changes to the manual.

DIT policies will be made available to all employees.

Managers must give new employees adequate time to review DIT policies and ask any questions during the employees' and contractors' first two weeks of work at DIT. At the end of the two-week period, employees must sign a statement acknowledging that they have been given the opportunity to review and ask questions about DIT policies.

1.14 LOSS, THEFT AND MISUSE OF STATE PROPERTY

Purpose

To establish a policy requiring DIT employees to report lost, stolen or misused state property.

Owner

Human Resources
Services Delivery

Policy

DIT employees must immediately report lost, stolen or misused property to their supervisor, who will forward the report to Human Resources.

The State CIO will report lost, stolen or misused property to the SBI as required by [G.S. 143B-920](#).

1.15 SEPARATION FROM EMPLOYMENT AND EXIT INTERVIEW

Purpose

To establish a policy for DIT employees to participate in an exit interview when being separated from employment with the agency.

Owner

Human Resources

Policy

When an employee separates from employment with DIT, an employee of DIT Human Resources must conduct an exit interview to:

- Determine the cause of turnover
- Ascertain that state property and equipment issued to the employee, including procurement cards, keys, ID badges, cellular phones and any other items, have been turned in
- Inform the employee about the various benefit programs.

Employees should provide a written letter of resignation at least two weeks before their expected separation date. The supervisor must forward a copy of any resignation or notice of retirement letter to DIT Human Resources.

Retiring employees should contact the Benefits Representative in Human Resources at least 90 days before retirement to discuss retirement benefits, longevity, annual leave pay, and complete the necessary paperwork.

All employees, whether resigning or retiring, should schedule an exit interview with the Benefits Representative in Human Resources before separating.

1.16 REDUCTION IN FORCE

Purpose

To establish policies and procedures for reduction in force that meet the needs of DIT, and provide assurance to employees that potential reductions shall be considered on a fair and systematic basis.

Owner

Human Resources

Policy

It is the intent of DIT to ensure that all employees have access to the Departmental Reduction in Force (RIF) procedures. The RIF policy will be evaluated and monitored continuously by the DIT Human Resources office.

DIT has the authority to separate an employee whenever it is necessary due to shortage of funds or work, abolishment of a position, or other material changes in duties or organization.

Retention of employees in affected classes shall be based on systematic consideration, at a minimum, of the following factors:

- Type of appointment
- Relative efficiency
- Actual or potential adverse impact on the diversity of the workforce
- Length of service

Neither temporary, nor probationary employees in their initial twelve months of employment, shall be retained in classes where employees with a permanent appointment (those who have satisfactorily completed a probationary or equivalent trial period) must be separated in the same or related areas.

In determining the length of service, an eligible veteran shall be afforded one year of state service for each year or fraction thereof of military service, up to a maximum of five years' credit.

Requirements

DIT shall develop written guidelines for reduction in force that meet its particular needs and provide assurances to employees that potential reductions shall be considered on a fair and systematic basis. These guidelines must be openly available for review by any employee of DIT at a publicized location.

This policy will be posted in a permanent and conspicuous manner in work areas and shall also be filed with NCOSHR as a public record.

EEO Compliance

DIT adheres to a philosophy of equal employment opportunity. When a RIF is necessary, all reasonable effort will be made to avoid adverse impact on the diversity of the work force. Section managers, along with the EEO Officer, shall review RIF recommendations before implementing them to determine the impact on the workforce and on the diversity of the work groups.

When an employee is separated due to a reduction in force, the EEO, Diversity & Inclusion Division of OSHR will conduct an efficiency evaluation.

DIT HR Responsibilities

The HR director must advise managers of existing staffing levels, vacant positions, and total classes assigned to DIT, and then monitor the RIF process to ensure compliance with State HR policies and all applicable statutes.

DIT HR staff will assist employees in requesting priority re-employment and determining their classification of interest before submitting their application to OSHR.

Section Manager Responsibilities

Section Managers must develop a written plan for a reduction in force as needed. This plan must meet section needs and ensure that reductions are implemented fairly and systematically. Each section's plan shall be available in the DIT HR Office for review by any DIT employee and will be filed with NCOSHR as a public record.

The Section Manager is the final authority for determining what positions will be eliminated.

Before section management determines which positions must be eliminated to satisfy mandated goals, they must pursue and exhaust all other alternatives. A RIF decision may be reached only after considering the following measures:

- Placing a hiring freeze on vacant positions
- Limiting purchasing and travel
- Changing retirement options
- Changing work options such as job sharing and alternative work schedules

When identifying positions for a reduction in force, managers must consider the following criteria:

- **Mandates to deliver specific services.**
- **Relative efficiency.** Section Managers must explore all possibilities on intra-departmental transfer where the employee shows potential to perform work in another organizational unit.
- **Length of service.** Length of service consideration applies only when employees with equal qualifications are being considered for reduction in force. In determining the length of service, an eligible veteran is accorded one year of State service for each year or fraction thereof of military service, up to a maximum of five years' credit.
- **Impact on workplace diversity (EEO considerations).** A reduction in force that creates or exacerbates an under-representation of any protected group must be avoided whenever possible. The EEO Officer will assess any proposed reduction in force for its impact on workforce diversity. The EEO Officer will analyze the impact of any reduction in force on the DIT demographic profile.

The Section Manager must give written notice of a reduction in force to affected employees as soon as possible; however, a minimum thirty-day notice of separation must be given. Official written notification letters should include the following:

1. Expected date of separation
2. Reasons for the reduction in force

3. Employee's eligibility to receive priority reemployment consideration
4. Applicable appeal rights
5. Other benefit information
 - a. Vacation pay
 - b. Sick leave

Appeals

An employee separated through a reduction in force may appeal the separation if it is alleged that the separation is in retaliation for the employee's complaint of alleged discrimination against the employee on account of the employee's age, sex, race, color, national origin, religion, genetic information, political affiliation, or disabling condition as defined by NCGS Chapter 168A.

An employee may appeal the separation if it is alleged that the separation constitutes a denial of the veteran's preference granted in connection with a reduction in force for an eligible veteran.

An employee who wishes to appeal a separation due to reduction in force through the internal grievance procedure must do so in writing within fifteen calendar days of notification of reduction in force to the DIT Human Resources Director.

Leave

Vacation Leave: Employees may elect, subject to approval by management, to exhaust vacation leave after their last day of work and be paid in a lump sum for the balance not to exceed 240 hours. If an employee had over 240 hours of vacation leave at the time of reduction in force, the excess leave shall be reinstated when reemployed within one year.

Sick Leave: Employees separated due to reduction in force shall be informed that their sick leave shall be reinstated if re-employed in any agency within five years.

SECTION 2 SECURITY

SITE SECURITY

2.1 FACILITY ACCESS

Purpose

To establish policy for site security at all DIT facilities.

Owner

Human Resources
Enterprise Risk and Security

Policy

Proper identification, authentication and authorization are required of all individuals attempting to enter a DIT facility. DIT may deny access to anyone who fails to comply with DIT security policies and procedures.

DIT employees performing their duties in non-DIT facilities must follow the site security policies of the agency where they are performing their duties.

DIT employees must use the NC Mail Center or P.O. Box address on all public documents, such as business cards, stationery and websites. The street address and/or directions to any DIT physical location should only be revealed in limited situations, such as when necessary for deliveries. The DIT street address also may be used in bid solicitation documents, announcements for bid openings and bidders' conferences.

With the exception of those in the possession of State Capitol Police, firearms are prohibited at all DIT locations.

DIT has the right to inspect any items entering or leaving DIT premises, and to refuse any item to be removed from or carried into its locations.

A violation of this policy may subject an employee to disciplinary action and may result in expulsion of contractors or others, in addition to legal actions.

DIT Badge Access

All DIT employees, contractors and visitors must wear DIT-approved badges in plain view at all times while in any DIT facility.

Badge requirements include the following:

- No one is to be permitted access to any DIT facility without proper authorization
- Anyone issued a badge has a responsibility to comply with DIT site security badge procedures and may be held responsible for improper badge use
- Any person with a DIT badge who knowingly uses the badge to admit a person without proper authorization into a DIT facility is in violation of the DIT site security policy and is subject to disciplinary actions
- Any lost or misplaced badges must be reported promptly to the DIT Capital Police officer or a security guard on duty and to Human Resources
- All green DIT employee badges and white contractor badges must be returned to Human Resources upon termination of the employee or contractor
- Human Resources must be notified promptly when an employee and/or third party has a change in status, including situations when an individual is terminated, transferred, suspended, or becomes inactive (i.e., no ongoing work related activities). It is imperative that inactive or terminated staff be disconnected from the badge system and other DIT systems on a timely basis. Transferred staff must have their access rights adjusted to reflect their new job duties.

The State CIO or a Deputy State CIO has final approval authority for all identification badges issued to DIT employees or contractors. Human Resources is responsible for issuing all badges and maintaining any forms, processes and procedures needed to carry out all badge policies.

Standards

Types of Badges

Green Badges – Permanent DIT Employees

Green badges with a photo will be issued to permanent DIT employees in accordance with this policy. Permanent DIT employees include legal counsel assigned by the Attorney General's office to represent DIT.

With the exception of the computer rooms at the Western Data Center and the Eastern Data Center, an employee's level of access within a facility is determined by the employee's manager and division director. Badge access to the computer rooms must be approved by the Chief Information Risk/Security Officer, or the officer's designee, in addition to the employees' manager and division director.

Temporary Green Badges – Permanent DIT Employees

Green badges without a photo ID, labeled TEMPORARY, may be issued to an DIT employee who has lost or forgotten his or her permanent badge.

To obtain a temporary green badge, the DIT employees must present a photo identification, unless they are known to the security guard on duty.

Employees with a green temporary badge must log in and out.

Temporary green badges must be returned to the Security Guard's Desk at the end of each working day, and may be used for up to five workdays. At the end of the five working days, an employee who has not found the permanent badge must pay for the cost of a replacement.

White Badges – State Employees and Approved Contractors

State employees who regularly have business at DIT facilities and contractors who perform work at DIT facilities may be issued a white badge.

A request for a white badge must be made by an appropriate DIT employee, as designated on the Facility Access Form.

A white badge issued to a state employee must include the user's agency. A white badge issued to a contractor must include the vendor's contract firm or the consultant company name abbreviated on the front of the badge. The badge must be returned to Human Resources at the end of the contract period.

White badges are authorized for periods not to exceed ninety (90) calendar days. Every 90 days, the DIT sponsor for the badge must verify that the badge access is still required.

Contractors with white badges must follow the procedures listed under Access Management below.

Background Investigations

Green DIT employee and white badges may be issued pending completion of a criminal background investigation conducted pursuant to [G.S. 143B-1336\(g\)](#). Badges may be revoked when the investigation is completed.

Red Badges – Visitors

All visitors and contractors not issued a white badge may be issued a red badge. Red visitor badges must be returned when the visitor leaves the facility.

All visitors with a red badge must be escorted by someone with either a green or white badge when in DIT facilities.

Procedures

Picture badge control and record keeping are the responsibility of the Human Resources Office.

A Facility Access Form must be completed by an employee's or contractor's supervisor for new badge access, a change in current badge access, and termination. Badge authorization forms may be obtained from the DIT Human Resources Office.

White badges for temporary employees, employees of other agencies and DIT contractors are processed and controlled in the same manner as for permanent employees.

Access Management

Visitors

Visitors and contractors without a white badge must present a photographic identification card, such as a driver's license or an employer issued identification card, to a guard at the Eastern or Western Data Center to receive a red visitor's badge. If no guard is on duty, the individual responsible for the visitor or contractor must verify the visitor's identification and provide a badge.

The guards, or a responsible individual if a security guard is not on duty, must require that all visitors and contractors without a white badge sign in and out.

Permanent DIT employees with green photo badges and persons with white badges are not required to sign in or out.

Children under 18 are not required to have an identification card but must be accompanied at all times by an adult who has a green or white badge.

Special Access Requirements for the Computer Rooms

Badge access to the computer room at the Western Data Center or Eastern Data Center must be approved by the Chief Information Risk/Security Officer or the officer's designee.

All persons must sign in to gain admission to the computer room, and must sign out when they leave, unless specifically granted approval for access without signing in. The sign-in sheets must include the person's name and affiliation.

Individuals required to sign in and out of the Computer Room must do so every time they enter and leave the Computer Room.

Summary of Badge Access and Escort Requirements

Badge Type	ID Required for Admittance	Log In/Out Required	Escort Required
Red	Yes	Yes	Yes
White	No	No	No
Green	No	No	No
Green Temporary	Yes, unless known by security guard	Yes	No

Additional Requirements for Staff

DIT staff is required to provide advance notice of expected visitors to the security guards or, if no security guard is on duty, the receptionist. If advance notice has not been given, the security guard or receptionist shall not admit the visitor until the DIT employee being visited has responded in person to the security guard or receptionist location to verify the identity of the visitor.

Nights, Weekends and Holiday Work Restrictions

With the exception of the computer rooms at the Eastern and Western Data Centers, DIT employees with green badges will be given general access to DIT facilities twenty-four hours a day, seven days a week. Access to the computer rooms is governed by ***Special Access Requirements for the Computer Rooms*** above.

State employees with white badges will have access to DIT facilities from 7 a.m. until 7 p.m. Monday through Friday. State employees with a white badge may be admitted to DIT facilities at other hours by a DIT employee with a green badge.

Contractors

Whenever there is no sponsoring permanent DIT employee to be responsible to escort and supervise a contractor's work during nights, weekends and holidays, access to DIT facilities will be denied. If essential work must be performed during these hours by contractors, someone from the division sponsoring the work must be available to escort the contractor.

The following information must be on file at the security guard station prior to the arrival of the contractor, or be provided upon the contractor's arrival:

- Name of person who will be working
- Specific areas to which access will be granted
- Name of sponsoring employee and/or DIT manager
- Phone numbers where sponsoring employee and/or DIT manager can be reached.

2.2 FACILITY ACCESS AFTER A CHANGE IN JOB DUTIES

Purpose

To require review of access to DIT facilities and assets upon a change in job duties that may require a different level of access.

Owner

Human Resources

Policy

Access to agency facilities, information, and other assets must be reviewed and changed accordingly upon a change in job assignments for an employee or contractor.

2.3 SEMI-ANNUAL BADGE ACCESS CERTIFICATION

Purpose

To regularly update badge authorizations to reflect changes in authorized facility access.

Owner

Human Resources

Policy

All DIT employee badge authorizations must be reviewed semi-annually to verify the correct level of facility access for each employee. This review shall be conducted by the DIT employee's manager and division director.

2.4 OBTAINING A BADGE ACCESS REPORT

Purpose

To establish policy on access to badge reports.

Owner

Human Resources

Policy

Reports generated by the badge access system, such as the time and location of a badge user's movements while at a DIT facility, are available to managers who specifically request them in writing. Such requests shall be addressed to Human Resources and shall be reviewed by the Human Resources Office.

INFORMATION SECURITY

2.5 GENERAL INFORMATION SECURITY

Purpose

To establish general policy and the information security framework for DIT.

Owner

Enterprise Risk and Security

Policy

DIT is subject to all information protection guidelines, principles, policies and standards established by the State Chief Information Officer (State CIO), including the [Statewide Information Security Manual](#), and the [Statewide Data Classification and Handling Policy](#).

With approval by the State CIO, DIT may implement and enforce security policies more stringent than enterprise risk and security policies.

Information, as defined by the [Statewide Glossary of Information Technology Terms](#), is data and records.

2.6 ACCEPTABLE USE

Purpose

To establish policy for acceptable use of information technology devices.

Scope

This policy applies to any DIT employee, contractor or third party who uses any device, whether state-owned or personal, to connect to the State Network. [G.S. 143B—1370\(a\)\(5\)\(g\)](#) defines the State Network as “any connectivity designed for the purpose of providing Internet Protocol transport of information for State agencies.” State law also requires the Department of Information Technology (DIT) to manage the State Network.

Owner

Enterprise Risk and Security

Policy

1. Users may not connect personal devices to the State Network without express written permission from the agency head or the agency head's designee. This requirement does not apply to users who connect to the State Network through a state-supplied "guest" Wi-Fi network.
2. Personally owned "smart" devices may not be connected to the State Network. "Smart" devices, commonly referred to as the "Internet of Things," include such devices as thermostats, wearable technologies, or appliances.
3. All devices connected to the State Network must have updated malware/anti-virus protection.
4. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.
5. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.
6. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e., Smartcard), or other similar information or devices used for identification and authorization purposes.
7. Users must not make unauthorized copies of copyrighted or state-owned software.
8. Users must ensure all files downloaded from an external source to the State Network or any device connected to the State Network, including a diskette, compact disc (CD), USB flash drive, or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code.
9. Users must ensure that the transmission or handling of personally identifiable information (PII) or other sensitive data is encrypted or has adequate protection.
10. Users may not download, install or distribute software to state-owned devices unless it has been approved by the agency head or the agency head's designee.
11. Users must not download state data to personally owned devices unless approved by the agency head or the agency head's designee.
12. Users must not purposely engage in activity that is illegal according to local, state or federal law, or activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene.
13. Users accessing the State Network through a Local Area Network (LAN) must avoid unnecessary network traffic and interference with other users. Specific prohibitions include, but are not limited to, the following:
 - (a) Unsolicited commercial advertising by public employees and State Network users. For the purpose of this policy, "unsolicited commercial advertising" includes any transmission initiated by a vendor, provider, retailer, or manufacturer of goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer that describes goods, products, or services. This prohibition does not include the following:
 - (i) discussions of a product or service's relative advantages and disadvantages by users of those products or services (unless the user is also the vendor, retailer, or manufacturer, or related to or affiliated with the vendor, provider, retailer, or manufacturer);
 - (ii) responses to questions, but only if such responses are direct replies to those who inquired via electronic mail; or
 - (iii) mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.
 - (b) Any other type of mass mailing by employees and others accessing the State Network through the agency LAN that does not pertain to governmental business or a state-sponsored activity.

14. Users accessing the State Network through an agency LAN must only access Internet-streaming sites as consistent with the mission of the agency for the minimum amount of time necessary.
15. Users must not engage in activity that may degrade the performance of information resources, deprive an authorized user access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.
16. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved in writing by the agency head or the agency head's designee.
17. Information technology resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
18. Access to the Internet from state-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to access nonpublic accessible information systems.
19. Users must report any weaknesses in computer security to the Department of Information Technology security liaison or designee for follow-up investigation. Weaknesses in computer security include unexpected software or system behavior, which may indicate an unauthorized disclosure of information or exposure to security threats.
20. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy.
21. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information.
22. Incidental use of the Internet is acceptable, provided that:
 - a) The use shall not negatively impact or interfere with an employee's work performance; or
 - b) The use does not result in costs to the state, legal action; or
 - c) The use does not violate other personnel or security policies, or negatively impact the Department.

Violations

Violation of this policy may result in disciplinary action, termination, loss of information resources and criminal prosecution.

Acknowledgement of Policy

Department of Information Technology employees and contractors must acknowledge in writing that they have received a copy of this policy. Written acknowledgement is also required annually on a date determined by Human Resources.

I have read, understand, and will abide by the Acceptable Use Policy when using computer and other electronic resources owned, leased, or operated by the Department of Information Technology. I will abide by the Acceptable Use Policy when using personal computing devices not owned, leased, or operated by the Department of Information Technology. I have no expectation of privacy when connecting any device to the State Network. Any violation of the regulations above may constitute a criminal offense. Should I commit any violation of this policy, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

User Signature

Date

2.7 NON-DIT MANAGED END USER DEVICES POLICY WITH TERMS AND CONDITIONS

Purpose

To establish requirements for end user devices that access the DIT LAN.

Owner

Enterprise Risk and Security

Policy

To protect DIT internal network from vulnerabilities that can be introduced when users access the State Network, DIT requires that all users adhere to required security configurations for those devices.

Failure to comply with this policy will result in denial of access to the DIT LAN and may result in disciplinary action.

Users of personal end user devices shall not circumvent security controls designed to protect registered devices and the DIT LAN.

Before being granted access to the DIT LAN, guests shall agree with and acknowledge receipt of the DIT Acceptable Use Policy.

Definitions

Authorized users – DIT employees and DIT authorized contractors who comply with this Policy.

End user device – A device, such as a laptop, smart phone or tablet that connects to the DIT LAN and that is owned by an authorized user.

Guest – Any person, including an employee of another state agency or a vendor who has been allowed to enter the DIT facility and has been provided with a guest account to access the DIT LAN.

Authorized User Terms and Conditions

Users shall be required to acknowledge and agree that:

- Users of personal end user devices shall not circumvent security controls designed to protect registered devices and the DIT LAN,
- DIT is not liable for any damages, including data or functionality losses, of an end user device that it authorizes an employee or contractor to use in the performance of his or her duties,
- DIT is not responsible for repairs, support or maintenance of any personal device used to connect to the State Network,
- Users shall comply with all statewide information technology policies and standards and all DIT policies, including the acceptable use policy, and
- DIT has the right to monitor the end user devices on the DIT LAN and to investigate reported incidents of suspected abusive and/or illegal activities on those end user devices. The investigations may include reviews of electronic data files and records on the end user devices.

Users shall be required to acknowledge and agree that a violation of any of these terms and conditions may result in appropriate disciplinary action.

Guest User Terms and Conditions

Guest users shall be required to acknowledge and agree that:

- Users of personal end user devices shall not circumvent security controls designed to protect registered devices and the DIT LAN
- DIT is not liable for any damages or loss of an end user device that it authorizes an employee or contractor to use in the performance of his or her duties
- DIT is not responsible for repairs, support or maintenance of any personal device used to connect to the State Network
- Guest users are responsible for maintaining all patches and anti-virus software on their devices and acknowledge that failure to maintain patches and anti-virus software shall result in denial of access

- Guests shall comply with the acceptable use policy and acknowledge that failure to do so may result in termination of access and liability for damages
- DIT has the right to monitor the end user devices on the DIT LAN and to investigate reported incidents of suspected abusive and/or illegal activities on those end user devices. The investigations may include reviews of electronic data files and records on the end user devices.

SECTION 3 WORKPLACE, HEALTH AND SAFETY POLICIES

3.1 USE OF STATE PROPERTY AND FACILITIES

Purpose

To establish general policies for the use of DIT facilities.

Owner

Human Resources

Policies

Use of DIT facilities is subject to state law and the following policies.

Celebrations

DIT employees may use conference rooms and dining areas for birthday celebrations, showers, retirement parties, etc., for DIT employees. Such events must be scheduled through the calendar system.

Bulletin Boards

Only those notices, brochures, bulletins, and pamphlets approved by Human Resources or the manager of the Western Data Center may be displayed on DIT bulletin boards. Persons wishing to display any of the above-mentioned items should submit their requests to one of the aforementioned sections.

The DIT bulletin boards are the only designated areas for displaying pamphlets and flyers. Attachment of notices, etc., to elevators, doors, or walls should be kept to a minimum and must be approved by Human Resources or the manager of the Western Data Center.

Division directors may approve items for posting on bulletin boards maintained for the use of employees in a specific division or section.

3.2 TORNADO AND SEVERE WEATHER WARNINGS

Purpose

To provide policy for responding to severe weather and tornado watches/warnings in the work place.

Policy

All DIT employees and contractors shall receive annual training on tornado and severe weather procedures. Upon notification of an alert, all employees and contractors shall follow the appropriate procedures.

3.3 FIRE SAFETY AND EVACUATION

Purpose

To establish a policy and procedure for the safe evacuation of DIT employees during fires or other natural disasters that require the evacuation of a building's occupants.

Owner

Human Resources

Policy

In an effort to ensure the safe evacuation of employees, contractors and visitors if a fire occurs at DIT, emergency evacuation drills will take place at least two times a year at all DIT facilities.

DIT will also establish fire evacuation plans to provide for the safe evacuation of all facilities during a fire or other natural disaster that requires evacuation to protect the buildings' occupants. To ensure compliance with this policy, DIT shall:

- Through a designated fire marshal, maintain up-to-date fire evacuation procedures for all buildings housing DIT employees
- Post exit information at appropriate locations
- Conduct unannounced fire drills and report the results of each fire alarm test with recommendations for improvement
- Place fire extinguishers in visible locations throughout DIT facilities.

DIT strictly forbids the use of personal heaters that contain flammable chemicals. Generally, the use of electrical heaters will not be allowed in DIT facilities, and should not be installed without the approval of the Facilities Manager.

3.4 BOMB THREATS

Purpose

To establish a policy and procedure for reporting and responding to bomb threats.

Owner

Human Resources

Policy

DIT employees must immediately report any bomb threat or suspicious package to on-site security staff or State Capitol Police.

The DIT Safety Officer, in conjunction with the State Capitol Police or on-site security staff, will develop procedures for evacuation or other action in the event of a bomb threat.

Training for DIT procedures regarding bomb threats must be included in the training provided to new employees and the annual security training.

3.5 SOCIAL DISTANCING POLICY

Purpose

To describe the authority of the State CIO during any communicable disease emergency.

Owner

Human Resources

Policy

Pursuant to the [OSHR Communicable Disease Emergency Policy](#), the State CIO may implement any directives issued by the Governor or any public health official during a public health emergency, or take any other action authorized by the state policy.

Specifically, the State CIO may require “social distancing,” as described in the statewide policy, to limit the spread of a disease by reducing the opportunities for close contact between people. The State CIO may also establish immediate telework arrangements, waiving the requirements of [DIT Policy 1.11](#).

Any actions ordered by the State CIO during a communicable disease emergency will be communicated immediately to DIT staff.

SECTION 4 ETHICS

4.1 ETHICAL STANDARDS: VENDOR GIFTS AND GRATUITIES

Purpose

To establish a policy for employee ethical standards.

Owner

Ethics Commission Liaison

Policy

Pursuant to [G.S. 143B-1353](#), DIT employees must not accept as gifts items of any value whatsoever from vendors who do business with the state, or who may do business with the state. This includes both IT and non-IT vendors.

In addition to the requirements of G.S. 143B-1353, all DIT employees are subject to the applicable provisions of the State Ethics Act, pursuant to [G.S. 143B-1322\(e\)](#).

A violation of [G.S. 143B-1353](#) is a Class F felony, and a DIT employee convicted of a violation may be terminated. It is also unlawful for vendors to provide gifts to certain state employees or for employees to accept such under [G.S. 133-32](#).

Employees must avoid any action that would create even the appearance that they are violating the law or ethical standards. DIT employees may not take any actions that give the appearance of favoring a particular vendor or group of vendors.

DIT employees must adhere to ethical standards, must not use their state position for private gain, and must not treat any private organization or individual unfairly.

DIT employees with questions about ethics policies should contact the DIT Ethics Commission Liaison. See [Appendix A](#) for guidelines.

4.2 MISUSE OF POSITION

Purpose

To prohibit DIT employees from using their position for private gain.

Owner

Human Resources

Policy

DIT employees must not use their public office for private gain. Employees are not to use their position, title, or any authority associated with their office to coerce or induce a benefit for themselves or others. This prohibition includes having a personal beneficial interest, whether direct or indirect, in a contract.

DIT employees also are not to use or allow the improper use of non-public information to further a private interest, either their own or that of another party.

4.3 SECONDARY EMPLOYMENT

Purpose

To require approval of secondary employment by DIT employees.

Owner

Human Resources

Policy

DIT employees are subject to the Office of State Human Resources policy regarding [Secondary Employment](#) and must obtain approval from the State CIO before engaging in any secondary employment.

DIT employees may not sell supplies or materials directly or indirectly to DIT, and may not work for anyone who is or may become involved in business with DIT.

4.4 DISCLOSURE STATEMENTS AND MANDATORY TRAINING

Purpose

To establish DIT policy on compliance with state ethics requirements.

Owner

Human Resources

Policy

The State CIO, Deputy State CIOs and others as designated by the North Carolina State Ethics Commission (Commission) must annually sign and file with the Commission all disclosures of financial interest and participate in ethics training as required by the Commission.

SECTION 5 PUBLIC RECORDS

5.1 PUBLIC REQUESTS FOR DIT RECORDS

Purpose

To establish a policy regarding public requests for records for which DIT is the custodian. Requests for records held by DIT for storage, safekeeping or data processing pursuant to [G.S. 132-6\(a\)](#), are governed by Policy 5.2, Public Requests for DIT Customer Records.

Owner

Legislative and Public Affairs

Policy

DIT will follow [N.C. General Statute Chapter 132](#) and other relevant statutes regarding public access to records.

DIT will not release confidential information except as allowed by law.

Only the DIT Director of Legislative and Public Affairs is authorized to provide records in response to public requests, with the exception of request for procurement file records after the award of a contract. [Policy 5.3](#) governs those requests.

5.2 PUBLIC REQUESTS FOR DIT CUSTOMER RECORDS

Purpose

To establish a policy regarding public requests for records for which DIT is not the custodian, but holds the records for storage, safekeeping or data processing pursuant to [G.S. 132-6\(a\)](#). Requests for records for which DIT is the custodian are governed by [Policy 5.1, Public Requests for DIT Records](#).

Owner

Legislative and Public Affairs

Policy

DIT will follow [N.C. General Statute Chapter 132](#) and other relevant statutes regarding public access to customer records.

When DIT receives a public records request for non-DIT records, the DIT Director of Legislative and Public Affairs will forward the request to the custodian of the records, and assist the custodian of non-DIT records in complying with the public records request. The Director of Legislative and Public Affairs must receive written authorization from the custodian of the records before providing access to or copies of any non-DIT or customer records.

Only the DIT Director of Legislative and Public Affairs is authorized to provide records in response to public records requests, with the exception of procurement records. In requests for procurement records, the Chief Procurement Officer is authorized to provide access or copies Pursuant to Policy 5.3.

5.3 ACCESS TO PROCUREMENT FILE RECORDS

Purpose

To establish a policy regarding requests for procurement file records.

Owner

Chief Procurement Officer

Policy

The Statewide IT Strategic Sourcing Office may handle, approve and schedule routine requests from vendors to review procurement file records.

Vendors may also make electronic copies of public information in procurement file records, using their own media, without filing a public records request.

[Policy 5.1 Public Requests for DIT Records](#) applies in all other requests regarding access to procurement file records, including requests for copies provided by DIT.

SECTION 6 PROCUREMENT

6.1 PROCUREMENT

Purpose

To set general policy for procurement by DIT.

Owner

DIT Procurement Administration and Facilities

Policy

DIT will comply with all state rules, policies and guidelines in procuring information technology, goods, and services.

Those include, but are not limited to, the [North Carolina IT Procurement Policies and Procedures](#) and the [North Carolina Procurement Rules](#).

SECTION 7 LEGISLATIVE AND MEDIA CONTACTS

7.1 LEGISLATIVE CONTACTS

Purpose

To establish a policy and procedures regarding interaction of DIT staff with members and support staff of the General Assembly.

Owner

Legislative and Public Affairs

Policy

Only DIT personnel designated by the State Chief Information Officer (State CIO) are authorized to appear before legislative committee meetings on behalf of DIT, or to provide information to members of the General Assembly or legislative staff.

Requests from legislators or legislative support staff for DIT staff to attend formal or informal meetings at the General Assembly must be reported immediately to the DIT Legislative Liaison. DIT staff must provide a brief description of the meeting and proposed remarks in writing to the DIT Legislative Liaison before the meeting.

In the case of requests for information from the member of the General Assembly or legislative staff, the division director and the Legislative Liaison, who will coordinate the agency's response.

If the request is marked "confidential" or is from the Program Evaluation Division, the DIT staff member receiving the request should contact either the DIT General Counsel or Attorney General's representative for guidance.

Procedure

Requests for information can generally be classified into one of three categories:

- 1) A request for a copy of previously published information.
- 2) A factual request. For example, how many State Network sites are there today?
- 3) A request for information regarding policy and or opinion, or a legal question. For example, is the public records statute clear?

For questions in category 1) or 2), DIT staff should immediately notify the DIT Legislative Liaison of the request and prepare a proposed response for review by the DIT Legislative Liaison prior to any submission to a member of the General Assembly or legislative staff.

For requests in category 3), DIT staff should direct the request to the division director, who should notify the DIT Legislative Liaison and the State CIO. If a written response is required, it should be reviewed by legal staff, appropriate DIT personnel and by the State CIO prior to sending it to the requester.

7.2 MEDIA CONTACTS

Purpose

To establish a policy regarding contact with the media.

Owner

Legislative and Public Affairs

Policy

All contacts from the media must be referred to the Director of Legislative and Public Affairs.

SECTION 8 INTERNAL AUDIT

8.1 INTERNAL AUDIT RESPONSIBILITIES

Purpose

To establish the role of DIT Internal Audit.

Owner

Internal Audit

Policy

Internal Audit is the point of contact for all external audits at DIT.

Internal Audit will lead the development of all agency responses to audit questions, findings and recommendations.

DIT Internal Audit shall develop an annual internal audit Charter and work plan.

<https://ncconnect.sharepoint.com/sites/it/docs/Documents/Internal%20Audit/ITS-Internal-Audit-Charter.pdf>

Internal audit's objective is to conclude whether the DIT internal control and governance processes, as designed and represented by management, are adequate and functioning in a manner to ensure:

- Programs are operating within the highest fiduciary standards and are directed toward the requirements defined in the federal and state laws, regulations, and rules, and statewide and DIT policies and procedures
- Programs and processes are consistent with industry best practices, using the best public and private examples as benchmarks
- Significant financial, managerial, and operating information is accurate, reliable, and timely
- Existing policies and procedures are appropriate and updated
- Operations, processes and programs are consistent with established missions, objectives and goals and whether they are being carried out as planned
- Risks within and outside DIT are appropriately identified and managed
- Quality service and continuous improvement are fostered in DITs' control process
- An effective system of internal controls that safeguards public funds and assets and minimizes incidences of fraud, waste, and abuse.

SECTION 9 ACCESS TO LEGAL COUNSEL

9.1 ACCESS TO LEGAL COUNSEL

Purpose

To establish a policy concerning access to legal counsel for DIT business.

Owner

Human Resources

Policy

The Attorney General's Office and the DIT General Counsel provide legal counsel to DIT. Any matter involving litigation or potential litigation should be promptly referred to the Attorney General representative representing DIT.

Before requesting advice of counsel on non-litigation matters, the employee should first review with his supervisor whether the issue actually involves a question of law.

All requests to the Attorney General's Office for an advisory letter or, the more formal, advisory opinion, shall be made in writing by the State CIO.

SECTION 10 DIT WEBSITE USAGE AND ACCESSIBILITY

10.1 DIT WEBSITE USAGE

Purpose

To restrict the use of DIT websites and links to public, non-commercial purposes.

Scope

This policy applies to the primary DIT website (<https://it.nc.gov>) and all websites maintained by DIT linked from that page.

Owner

Legislative and Public Affairs

Policy

DIT websites and links from DIT websites may only be used for public purposes. They may not be used to promote any commercial activities or to provide a public forum.

DIT will not promote or endorse any products, vendors or consultants on its websites, and nothing on DIT websites, or in external links, may suggest or imply any such promotion or endorsement. Any mention of vendors, products, or services shall be limited to informational purposes only.

DIT websites may not link to any external site that utilizes or serves any tool or technique that attempts to compromise the security of a user's access device or that increases the security risk to the DIT site in any way.

Links to external sites from the DIT website will not display content from those sites within DIT frames or borders or use any other method to display such content that may create confusion about the origin of the content or imply that DIT has control or endorsement of the content.

10.2 WEBSITE ACCESSIBILITY

Purpose

To require DIT websites that are accessible to people with disabilities.

Owner

Online/Digital Technology Director

Policy

In developing DIT websites, designers must consider the recommendations in [Web Content Accessibility Guidelines 2.0](#) (WCAG 2.0) to make the sites more accessible to people with disabilities.

The four principles of WCAG 2.0 are:

- **Perceivable** - Information and user interface components must be presented to users in ways that they can perceive, regardless of the user's functional impairment
- **Operable** - user interface components and navigation must be operable, regardless of the assistive technology used to interact with the interface
- **Understandable** - information and the operation of the user interface must be predictable and understandable to the user
- **Robust** - content must be robust enough to be able to be transformed and interpreted by a wide variety of user agents, like assistive technologies.

Accessibility Handbook

Web and content developers are encouraged to consult the [N.C. State University Web Accessibility Handbook](#) for guidance in creating accessible websites and digital interactions.

SECTION 11 RECORDS RETENTION

11.1 RECORDS RETENTION

Purpose

To establish policy for the retention and destruction of records for which DIT is the custodian.

Owner

DIT Chief Records Officer

Definitions

The [General Schedule](#) addresses records commonly found in agencies throughout state government, provides uniform descriptions and disposition instructions, and indicates minimum retention periods.

The [Program Records Schedule](#) lists program-specific records maintained by DIT.

Policy

DIT will follow state law, including [GS 132-3](#), administrative rules, and the [requirements of the Government Records Section \(GRS\)](#) of the [Department of Natural and Cultural Resources](#) in retaining and disposing of public records.

DIT will adopt a General Records Schedule and any program record schedules that are needed. All records schedules must be reviewed annually by each division or section, in conjunction with the Chief Records Officer, to ensure compliance with federal, state and DIT requirements.

DIT will comply with Executive Order No. 12 in the handling and disposition of email records. One of the requirements of the Executive Order is that emails be retained for at least five years.

Chief Records Officer

The State CIO will designate a DIT employee as the Chief Records Officer (CRO) for the department. The CRO serves as the primary point of contact with the Government Records Section (GRS) and coordinates all agency requests for records assistance and records training with the GRS. The Chief Records Officer also acts as agency coordinator for all records activities, programs, and reports required by the Department of Cultural Resources in administering the state records management program.

Each Deputy State CIO within DIT, the Human Resources Director, the Director of Enterprise Risk and Security, the Chief Financial Officer and any other manager designated by the CRO must designate one or more DIT employees to serve as Records Liaisons who work in conjunction with the CRO and the Government Records Section to establish retention schedules. Each Records Liaison should be an agency employee with detailed knowledge of the operations and records of a division or section.

When an employee serving as a Records Liaison is transferred or ceases employment with DIT, the Deputy State CIO for the liaison's division must assign another employee to manage the records, and notify the CRO of the change in personnel.

SECTION 12 BUDGET AND FISCAL POLICIES

BUDGET POLICIES

12.1 BUDGET DEVELOPMENT AND EXECUTION

Purpose

To establish general policy for the development and execution of DIT's budget.

Owner

Budget and Finance

Policy

DIT follows the policies and procedures in the [State Budget Act](#) and applicable sections of the [North Carolina Budget Manual](#) to develop, execute and report on the department's budget.

The N.C. Integrated Budget Information System (NCIBIS) must be utilized for budget execution for revision, allotments and certification.

NCIBIS also must be utilized in budget development for any Work Sheet I, Work Sheet II and Work Sheet III.

FISCAL POLICIES

12.2 STATEWIDE FISCAL POLICIES APPLY

Purpose

To establish general fiscal policy for DIT

Owner

Budget and Finance

Policy

DIT Budget and Finance follows all statewide fiscal policies established by the Office of State Controller and the Office of State Budget and Management.

OFFICE OF STATE CONTROLLER FISCAL POLICIES

[100 Accounting and Financial Reporting](#)

[200 Accounts Receivable](#)

[300 Cash Management](#)

[600 Foreign Nationals](#)

[700 HR/Payroll](#)

[800 Systems Security](#)

[900 Internal Controls](#)

[1000 Overpayment Audit](#)

[1100 State Disbursing](#)

[1200 Tax Compliance](#)

OSBM FISCAL POLICIES

[State Budget Manual Fiscal Policies and Regulations](#)

SECTION 13 POLICY MANUAL REVIEW AND UPDATES

13.1 POLICY AND PROCEDURES REVIEW AND REVISION PROCESS

Purpose

To establish policy for updating the *DIT Employee Manual*.

Owner

DIT Policies and Procedures

Policy

Policy owners will review the *DIT Employee Manual* at least annually and update as needed.

Procedures for reviewing, adding, revising or deleting policies will be developed by the DIT Policies and Procedures team and approved by the State CIO.

DIT Senior Leadership and others who may be affected must be given an opportunity to review any proposed changes to the *DIT Employee Manual*.

Emergencies

The State CIO may approve changes or additions to the *DIT Employee Manual* outside the normal review and approval process in cases of emergencies. Any changes will be immediately communicated to those affected.

Minor Changes

The DIT Policies and Procedures team may correct spelling, grammar, and punctuation in the *DIT Employee Manual* at any time. The team may also rearrange the policies and renumber them, if necessary.

When an agency re-organization occurs, the DIT Policies and Procedures team must review the manual and develop, with the policy owners, recommended ownership changes.

Ownership changes resulting from a DIT reorganization may be approved outside the normal policy approval process, but must be approved by the appropriate Deputy State CIO and the State CIO.

Notification of Changes or New Policies

All approved revisions will be incorporated into this manual as soon as possible after approval, and those affected will be notified by email or other means if the change is significant in the view of DIT Policies and Procedures or senior leadership.

General information about the State Ethics Act is available on the [N.C Ethics Commission website](#).

Gifts

Pursuant to [G.S. 143B-1353](#) and [Policy 4.1](#), DIT employees must not accept as gifts items of any value whatsoever from vendors who do business with the state, or who may do business with the state. This includes both IT and non-IT vendors. Items that may not be accepted include, but are not limited to, trinkets, free seminars, training, meals, etc.

If a vendor offers a gift or any item for free to a DIT employee, including trinkets, the employee must either decline it or pay full market value for it. If it is paid for and it is a vendor-specific trinket, it may not be displayed in the work place.

If an employee receives a gift from a vendor without the opportunity to decline it immediately, the employee must return the gift or pay its market value to the vendor. If the gift is perishable and it is not practical to return it, the gift may be given to a charity designated by the state or disposed of with a witness. This must be reported in writing to the employee's supervisor or the DIT ethics officer. If the gift is given to a charitable organization, a letter donating the gift must be placed on file with the State CIO's office.

If there is an existing relationship between an DIT employee and a vendor that includes the customary exchange of gifts for personal occasions, this policy does not prohibit that interaction. The gift shall not in any way be from the vendor company itself and shall not reflect the vendor company.

Training/Seminars/Events

To avoid the appearance of impropriety, employees cannot attend free training seminars or events to which they are individually invited. However, DIT recognizes the value and importance of these seminars to our business. Therefore, the following options exist:

If the employee's supervisor determines that the training, seminar, or event will be valuable to the employee, then the supervisor may decide to pay for the training or seminar. The supervisor shall send a direct pay form to the DIT Accounts Payable Manager along with a completed form letter to be sent to the vendor with the check. Payment may also be made by procurement card.

Once the seminar is fully paid for, it no longer falls within this policy and items that are distributed as part of the training or seminar may be accepted. Vendor-specific trinkets may not be displayed at DIT.

If the vendor sends an invitation to the state inviting state employees (not specific individuals) to attend training, a seminar, or an event, the state may accept the cost of the event as a donation. The state and the vendor shall sign a letter of agreement laying out the terms of the donation (specifically, that the vendor does not expect anything in return and the state will not give the vendor preferential treatment). Then, the state may choose specific individuals to attend the training, seminar, or event. Employees may then fully participate in the training, seminar, or event including eating food that is provided to all seminar attendees. The State CIO or designee is responsible for coordinating these efforts and ensuring the appropriate documentation is in place.

Employees may attend public or community events even if sponsored by vendors when the event is generally open to the public or when the employee is invited in clearly a community or non-work capacity. This includes events sponsored by or in conjunction with a civic, charitable, governmental, or community organization. If the event requires the purchase of tickets, DIT employees may not accept gifts of free tickets from vendors.

Employees may not attend work-related events that are primarily social in nature for which either the employee or DIT did not pay a fair market registration fee and which are sponsored (paid for) by vendors (one or more) which do business with the State of North Carolina. This includes social events sponsored by a vendor or vendors.

Employees may accept invitations to speak on work-related topics at vendor hosted conferences. They may not accept payment for this service, but they may accept travel expenses and do not need to pay to attend the particular event at which they are speaking. However, if they are attending an entire conference or convention, the individual or the state shall pay the conference fee.

Conferences hosted by professional organizations that do not function as a vendor to the state may provide travel expenses, waive conference fees and provide meals for DIT employees whose attendance has been approved by the State CIO or a Deputy State CIO.

Employees required to file a Statement of Economic Interest (SEI) by G.S. 138A, the State Government Ethics Act, must report any conference expenses paid by a professional organization as a scholarship on the SEI.

Individual Meetings

If a vendor requests a meeting with a DIT employee to provide business information or an employee requests information from a vendor, whether in the form of a formal presentation or a one-on-one meeting, this is consistent with standard business practices and is acceptable. Employees may not accept gifts or trinkets during the meeting and if the meeting includes a meal, employees must pay for their own food.

Hardware/Software

Employees may not accept free hardware or software from vendors.

If a vendor wants to provide test or demo software or hardware to DIT for a specified and reasonable period of time, this is acceptable; however, hardware and software must be returned to the vendor (and, in the case of software, deleted from any hardware) after the test period. This testing period shall not be used as a substitute for a project pilot either internally or for customers. Employees must clear acceptance of test or demo software or hardware with their supervisor who will determine, in consultation with DIT Purchasing, if a purchasing order is necessary. Employees cannot accept an obligation to purchase as part of a trial agreement outside of the purchasing process. When equipment is returned, DIT purchasing shall be notified by the requestor to close the zero-dollar purchase order. While it is the responsibility of the individual employee to return these items, DIT will conduct spot audits to ensure compliance with this policy.

Vendors can provide demos to DIT employees of their software or products that reflect specific requirements defined as part of an information gathering activity. This includes free demonstrations offered over the Internet.

DIT will not accept vendor offers of free customized software, services, or hosting services to use as a pilot or to provide a service to customers unless offered in response to a DIT purchasing solicitation.

If software is widely available to the public (e.g., can be downloaded through the Internet) and a vendor suggests an employee take advantage of this software, this is not considered to be a gift. If a vendor makes software available as part of a contractual relationship (e.g., they have updated their help desk support which is included in the contract and new software is needed to support it) this is not considered a gift if it is routinely provided to other customers at no charge.

Meals/Food

Employees shall not accept meals paid for by vendors.

If an employee is in a situation where it becomes impossible to turn down an offer of food or to pay for it, the employee must document this instance and report it to the DIT ethics officer or his immediate supervisor.

DIT employees may dine with vendors; however, they may not accept a vendor offer to pay for the meal.

Marketing Materials

Should DIT employees routinely receive marketing information delivered to them either as a result of mass mailings or in response to a direct request for information, these materials shall be discarded after their reference value has expired.

Exceptions

If an employee is at a conference or event for which the state has paid full market value, employees are entitled to take trinkets, demo diskettes, videos, etc., if they are included as part of the conference materials. However, employees may not bring vendor-specific trinkets into the work place. Employees may not enter their names for door prizes or other drawings. Employees may attend and participate in events that are a part of the conference, including hospitality suites, if the events are open to all conference attendees.