State of North Carolina
Department of Public Safety
POLICIES & PROCEDURES

HUMAN RESOURCES

Division:	ADMINISTRATION
Chapter:	HUMAN RESOURCES
Procedure:	HR/PAYROLL SYSTEM ACCESS GUIDELINES
Issue Date:	JUNE 1, 2016
Revised:	JANUARY 1, 2018

Preface

Within the Integrated HR/Payroll System, there are standard security roles. A role is a set of transactions, tasks, and/or responsibilities that serve a specific purpose or function. Employees may have a variety of duties and responsibilities, many of which require HR/Payroll System access. While access is assigned based on the duties of the position, there are several standard categories of users, each with a specific set of security roles. Each role is further limited by the security level for the position, i.e., work unit, facility, district, region, division, etc. It is important to remember that roles are assigned to positions and not employees. The roles remain with the position and only change if the duties and responsibilities of the position change.

Categories of Users

Super users:

This includes employees occupying positions with primary responsibility for Human Resource (HR) and Payroll Administration including employment processing and in some cases possessing approving authority. The positions are located in the Central HR Office, the Regional Employment Offices (REO) and the Controller’s Office. These users are assigned a combination of roles based on specific HR or Payroll Administration duties.

Core users:

This includes employees occupying positions outside of HR and/or the REO, but with a responsibility for maintaining employee data. These positions may be assigned the following security roles:

Display Benefits
Display Payroll
Display Organizational Management
Display Non-sensitive HR data
Display HR Director
HR Master Data Maintainer Lite
Time Administration/Display Time
Leave Administration
FMLA Event Maintainer

Time Administrators (Timekeepers):

This includes employees occupying positions with the responsibility for maintaining time records in the HR/Payroll system to include entering hours worked and leave taken. These positions are assigned the following roles:

Display Time
Time Administration

Depending on the location, some positions are also assigned an extra time role such as Leave Administration and/or FMLA Event Maintainer.

Managers:

Those individuals with management responsibilities may only need display roles in the HR/Payroll system. These roles allow individuals to view data but not process changes or actions. These users may be assigned the following roles:

Display HR Director
Display OM
Display Non-sensitive HR Data
Display Salary and Pay Grade
Display Performance Ratings
Display EEO
Display Warnings
Display Time

Depending on the location and whether the work unit/facility is using Employee Self Service/ Manager Self Service, some managers may have been assigned additional roles, such as Time Approver, or may not have all of the above listed roles.

Security Role Names

HR Master Data Maintainer

The functions of the HR Master Data Maintainer are assigned to employees in the Central HR Office and the REO's only. This role is responsible for processing employment actions, including new hires, separations, promotions, demotions, reassignments, reallocations, transfer, leave of absence and return from leave of absence.

HR Master Data Approver

HR Master Data Approvers are those employees in the Central HR Office and the REO's with the security level to approve employee actions, including new hires, separations, promotions, demotions, reassignments, reallocations, transfers, leave of absence and return from leave of absence.

HR Master Data Maintainer Lite

This is an abbreviated role that may be assigned to employees outside of Central HR and the REO's with HR responsibilities. This role allows the user to maintain/update specific employee data for employees within the designated work unit.

Time Administrator

Employees designated as Time Administrators (timekeepers) are assigned the Time Administration and the Display Time security roles. This role is responsible for entering hours worked and leave taken for employees, reviewing time evaluation results, and supporting the management of substitutions and on-calls. This role also has the ability to make corrections on electronic timesheets that have already been approved.

Time Approver

This role allows for the user to approve time entered via ESS in the absence or unavailability of the supervisor/manager who is normally responsible for approving time in Manager Self Service (MSS).

Leave Administrator

The Leave Administrator role manages leave balances. This role has the ability to make adjustments to absence quotas for advanced leave and manages FML, FIL, CSL options and can manage shared leave. This role can also review leave balances and make manual adjustments if a discrepancy exists. The Time Administrator/Time keeper cannot perform this task (unless he/she has both roles).

FMLA Event Maintainer

The FMLA Event Maintainer role establishes and maintains FML events, dates, reasons and generates FML records used by the Leave Administrator to designate specific absences as FML.

OM Position Approver and OM Position Requestor

These roles are assigned to the Classification Staff in the Central HR Office and a select group of employees in the divisions with specific responsibilities that require that the roles be assigned.

OM Supervisor Maintainer

This role is limited to DPS and allows the user to make changes to the supervisor/ subordinate relationship in the HR/Payroll System. This role is only functional if the user also has the HR Master Data Maintainer Lite security role and the organizational unit has been collapsed.

Grievance Maintainer

This role is only assigned to a select number of positions in the HR Office and EEO Staff.

Warnings Maintainer

This role is only assigned to a select number of positions in the HR Office and EEO Staff.

Short-Term Disability Specialist

This role is only assigned to a select number of positions in the HR Office.

The Agency Position Funding Approver security role is only assigned to agency Budget employees and the Payroll Administration security role is only assigned to DPS Payroll employees.

HR/Payroll Security Requests - General Information

HR/Payroll System Security Roles are assigned to a position by the Office of State Controller (OSC) Security Team in response to a request from an Agency Data Owner. Only the agency Data Owner is authorized to submit requests for HR/Payroll System security. Security is further limited by the organizational unit to which access is requested and granted. While security is not assigned to an employee, personnel changes can impact a position’s security. When a position is vacated, some security roles will be delimited. Therefore, when the position is filled, a security request must be submitted by the Agency Data Owner. The roles that do not require training will be reactivated upon receipt of the request. Roles that require training will be activated after the employee completes any required training.

Some positions will have no HR/Payroll System security history. A security request is required as with any other position, but may require additional justification supporting the request.

Reasons Precipitating the Need for a Security Request

A request for HR/Payroll System security is submitted to the Agency Data Owner in the HR Office under the following circumstances:

1. Changes to the occupant of a position;
2. To add an HR/Payroll System security role;
3. To remove an HR/Payroll System security role;
4. To change the organizational unit to which the security has been set;
5. When a new position is established;
6. Change in the duties of a position/employee.

Requests for Security Changes

Requests for security may be initiated by the work unit, but shall follow the chain of command through the unit and section manager for review and approval. The request shall be submitted by electronic mail. Information to be included in the request to the Agency Data Owner includes:

1. Full Employee Name
2. Employee HR/Payroll System Personnel Number
3. SAP Position Number to which security will be attached
4. Position Title
5. Security Roles/Organizational unit name and number for which security is to be added or removed
7. Detailed explanation for the requested security
8. Approvals from the Supervisor, Manager and/or other responsible staff.
9. Whether the request is for permanent access or temporary access and if temporary, the beginning and ending date.

Temporary Security Changes

Changes to security can also be done on a temporary basis with a pre-set deadline. However, it is noteworthy that if this is done, the security will expire on the specific date selected as the deadline. It is important that users are aware if security has been granted temporarily so they can anticipate the deadline and an extension can be requested by management to the agency data owner if necessary.

Agency Data Owner Procedures

Upon receipt of a request for HR/Payroll System security, the Agency Data Owner will review the request in consideration of the below listed criteria to determine if the request can be fulfilled.

1. Did the request follow the appropriate chain of command? Where did the request initiate and who submitted the request? i.e., Employee, Supervisor, or Manager? Employees may not submit requests for their own security/position.
2. What roles and level of security are being requested?
3. What is the position and what are the job duties for which the request was submitted?

4. What is the explanation for the request? Does it fit the job duties and responsibilities?
5. What pre-approvals are required for the request and are those included?
6. Will it require a Segregation of Duty Risk Acceptance form?
7. Is the request different from the existing security attached to the position? If so, is there an explanation for the deviation?
8. Is it a request to remove roles or limit security?
9. Is it permanent or temporary? If temporary, what are the effective and expiration dates?

Approvals Required

Requests from employees for changes to their own position shall be referred to the supervisor and manager for approval.

Requests for security beyond the org unit to which the employee is assigned and/or has HR functional responsibility shall be referred to the supervisor and manager for approval. For example, a request to give time administration to a position at Central Prison for a Highway Patrol Troop requires an explanation and approval from both section managers.

Certain security roles will require review and approval by management. The agency data owner will refer the request as necessary to the appropriate manager as listed below.

Role Name	**Required Approval Level**
HR Master Data Maintainer/Lite	HR
Time Administration	Work Unit Manager
Agency Position Funding Approver	Controller
OM Position Requestor	HR
HR Master Data Approver	HR
OM Position Approver	HR
OM Supervisor Maintainer	Work Unit Manager
Leave Administrator	Work Unit Manager
FMLA Event Maintainer	Work Unit Manager
Note: The FMLA Event Maintainer is dependent upon the Leave Administrator role.	
Short Term Disability Specialist	HR
Time Approver	Section Manager
Note: This role is only needed for work units that use ESS with Time	
Payroll Administration	Controller
Display HR Director	Work Unit Manager
Grievance Maintainer	HR Director
Warning Maintainer	HR Director
Display Non-Sensitive	Work Unit Manager
Display Salary and Pay Grade	Work Unit Manager
Display Payroll	Work Unit Manager

Display Performance Ratings	Work Unit Manager
Display Time	Work Unit Manager
Display Warnings	Section Manager
Display Grievances	Section Manager
Display EEO	Work Unit Manager

BOBJ Reports

The BOBJ reports are associated with the different roles. However, access to reports can also be requested without having the associated role and are subject to the same process and evaluation as other security roles.

Approvals, Denials and Processing

If the request is for job related reasons, includes the necessary approvals and is within these guidelines, the Agency Data Owner shall submit the Security Request to BEST electronically.

If the request cannot be fulfilled as requested, the Agency Data Owner shall notify the requestor and include the reason for the denial and what, if any changes are possible that would allow the request to be processed. The HR Director shall also be notified of any denials.

Training

The required training will populate in the employee's transcripts in Learning Management System (LMS), based on the requested roles.

HR/Payroll System Security roles that require training for access will be delimited when a position is vacated. HR/Payroll System Security roles that do not require training by OSC will be accessible, however, training is still required by DPS. Training may be web-based, virtual classroom or in-person instructor lead. The classes needed by the employee for the requested HR/Payroll System security roles will populate in the employee's LMS transcript. The employee will be able to request, register and schedule the classes through the LMS. Upon completion of all required training, within five business days the security analyst with OSC will be notified and the security will be activated for the position.

Training is provided for all HR/Payroll System security roles; however, some roles require training before the security request will be processed by the OSC Security Team. Those roles include:

HR Master Data Maintainer (Only assigned to Central and REO HR staff)
HR Master Data Approver (Only assigned to Central and REO HR staff)
HR Master Data Maintainer Lite
Time Administration

OM Position Requestor and OM Position Approver (Only assigned to Central, REO HR Staff and employment specialists with NEO Gov responsibilities for posting positions).

There are specific classes assigned including prerequisites for each of the above roles. The system is designed to prevent an employee from registering and scheduling classes where they have not successfully completed the prerequisite.

The HR Master Data Maintainer Lite security role is unique to DPS therefore, the assignment of this training is managed differently. The required classes for this security role include the PA210 and the PA315. Both are web-based classes. Upon approval and submission of the security request by the DPS Data Owner, the OSC Training Team is notified of the request. The OSC Training Team will first verify that the employee has successfully completed the PA210 Class prior to assigning the PA315 Module to the user's transcript. The PA315 Module is designed to take approximately four hours providing time for each student to go through the exercises thoroughly. The guidelines for this particular class are very strict as it is directly tied to the Master Data Maintainer Lite Role. Therefore, if a student does not view the tutorial at least the duration of the presentation, two hours and 53 minutes AND achieve 80% or above on the assessment, the employee will not be given access. There will be NO exceptions to this rule.

Since this is a WBT, the student can start and stop this presentation as often as they need to as it is self-directed. **OSC will monitor every student's time and IF THE STUDENT DOES NOT SPEND AT LEAST THE 2 HOURS AND 53 MINUTES VIEWING IT, THEY WILL NOT BE GIVEN ACCESS EVEN WITH A PASSING SCORE.**

In all cases of any required training that includes an assessment, the user will be given TWO attempts to pass the assessment. If it is not passed by the second attempt, a reevaluation of the request shall be required and the employee will not be granted the access to the security role.

A request for a reevaluation must be submitted to the DPS HR Regional Training Manager for DPS Central HR Office for review and approval before any further training and/or attempts will be allowed.

Once the employee has **successfully** completed all training and the assessment, the security request will be processed and access granted.

January 1, 2018 Updated Training Section to incorporate procedures for the PA315 class.