


CITY OF CATHEDRAL CITY ADMINISTRATIVE POLICY			HR-AP 19
TOPIC	EMAIL AND CELL PHONE ACCESS POLICY		
Approved by:		Distributed by	Original Date
 <small>Charles McClendon City Manager 2024-11-29 09:01</small> Charles McClendon, City Manager		Human Resources	July 18, 2024
			Revised

Subject

Email and Cell Phone Access Policy for IT and Department Heads

1. Purpose

This policy outlines the procedures and guidelines for accessing city-issued email accounts and cell phones for legitimate business purposes, such as investigating potential misconduct, responding to legal requests, or ensuring continuity of operations.

2. Scope

This policy applies to all city-issued email accounts and cell phones and applies to all employees, contractors, and authorized personnel who may require access to these accounts.

3. Authorized Access

3.1. Access to city-issued email accounts and cell phones shall be granted only to authorized personnel, such as the IT Department, Human Resources, or designated managers, on a need-to-know basis.

3.2. Authorized personnel must complete a Request for Access to City-Issued Email and Cell Phone Account for approval from their department head or the City Manager before accessing any city-issued email account.

3.3. Access shall be limited to the minimum necessary scope and duration required for the legitimate business purpose.

4. Legitimate Business Purposes

Authorized access to city-issued email accounts may be granted for the following legitimate business purposes:

- 4.1. Investigating potential misconduct or violations of city policies or laws.
- 4.2. Responding to legal requests, such as subpoenas, court orders, or public records requests.
- 4.3. Ensuring continuity of operations, such as accessing critical information in an employee's absence or during an emergency.

4.4. Conducting routine system maintenance, backups, or security monitoring.

5. Procedures

5.1. The requesting party shall submit a written request to their department head or the City Manager, stating the legitimate business purpose, the specific email account(s) and/or cell phone to be accessed, and the desired scope and duration of access.

5.2. Upon approval, the IT Department shall grant access to the authorized personnel and maintain a log of all access activities.

5.3. Authorized personnel shall access the email account(s) and or cell phone only for the approved purpose and shall not disclose or use the information for any other purpose.

5.4. Any sensitive or confidential information accessed shall be handled in accordance with applicable laws, regulations, and city policies.

6. Monitoring and Auditing

6.1. The IT Department shall implement appropriate logging and auditing mechanisms to track and monitor access to city-issued email accounts.

6.2. Human Resources shall conduct regular audits to ensure compliance with this policy and to identify potential misuse or unauthorized access.

7. Violations and Disciplinary Actions

7.1. Unauthorized access or misuse of city-issued email accounts may result in disciplinary action, up to and including termination of employment or contract, and potential legal consequences.

7.2. Suspected violations of this policy shall be reported to Human Resources and the City Manager for investigation and appropriate action.

8. Policy Review and Updates

This policy shall be reviewed and updated periodically to ensure compliance with applicable laws, regulations, and best practices.

By implementing and adhering to this policy, the city aims to strike a balance between legitimate business needs and the protection of employee privacy and data security.

Request for Access to City-Issued Email and Cell Phone Account

REQUESTOR INFORMATION:

Name:	
Department:	
Job Title:	
Date of Request:	
Access to the following individuals:	

EMAIL ACCOUNT(S) TO BE ACCESSED:

City Issued E-mail	City Issued Cell Phone

LEGITIMATE BUSINESS PURPOSE (SELECT ONE):

Identify	Cause	Detailed Justification for Access
	*Investigating potential misconduct or policy/law violations.	
	Responding to legal requests (subpoenas, court orders, public records requests)	
	Ensuring continuity of operations (employee absence, emergency)	
	Routine system maintenance, backups, or security monitoring	

REQUEST SCOPE OF ACCESS

Identify	Access	Duration
	Full access to emails, calendar, contacts	
	Limited access to specific folders/labels:	
	Access to emails within a specific date range:	_____ to _____

By signing below, I acknowledge that I have read and understand the Email and Cell Phone Access Policy, and I will access the requested email account(s) solely for the legitimate business purpose stated above and within the approved scope and duration. I will handle any sensitive or confidential information accessed in compliance with applicable laws, regulations, and city policies.

Requestor Signature: _____ Date: _____

*Human Resources : _____ Date: _____
- *Required for Investigating potential misconduct*

FOR DEPARTMENT HEAD/CITY MANAGER USE ONLY:

Request Approved Request Denied

Authorized By: _____ Date: _____
(Department Head or City Manager)






HR-AP 19 Email Access Policy Final

Final Audit Report

2024-07-17

Created:	2024-07-17
By:	Eugenia Torres (hr@cathedralcity.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAdxrqQO47WidRFW_L5OW00iatffKy344a

"HR-AP 19 Email Access Policy Final" History

-  Document created by Eugenia Torres (hr@cathedralcity.gov)
2024-07-17 - 0:56:59 AM GMT
-  Document emailed to Charles McClendon (cmclendon@cathedralcity.gov) for signature
2024-07-17 - 0:57:29 AM GMT
-  Email viewed by Charles McClendon (cmclendon@cathedralcity.gov)
2024-07-17 - 0:57:39 AM GMT
-  Document e-signed by Charles McClendon (cmclendon@cathedralcity.gov)
Signature Date: 2024-07-17 - 6:36:07 PM GMT - Time Source: server
-  Agreement completed.
2024-07-17 - 6:36:07 PM GMT