DECISION BRIEF **SUMMARY SHEET**	
Title: 2019.02 ER DOJ POL Info Sec DB	
Initial Requester: Matthew Grimm	**Contact Information:** MGrimm@mt.gov
Submitted By (SITSD Rep): Joe Frohlich	**Contact Information:** jfrohlich@mt.gov
Action Requested: Request - Exception	**Entity Impacted:** DOJ

Brief Description and Recommendations:
Matt Grimm from DOJ submitted an exception request to the POL-Electronic Mail Policy to re-direct emails from mt.gov's accounts to non-state email addresses. The management team must review, make suggestions and decide on this request.

If applicable, please include:

☒ ServiceNow documentation included and case # SCTASK0015801
☐ ITPR documentation included and case # Click here to enter case number.
☒ Policy included

Check all that apply:

☒ Internal Communication Required
☐ External Communication Required
☐ Enterprise Information Technology Financial Workgroup Review Required

Administrative Use Only

Publish Date: 2/14/2019	**Response Deadline:** 2/21/2019

RECOMMENDATION
CIO DECISION

☒ Recommendation Approved	☐ Recommendation Disapproved
☐ Recommendation approved with changes as noted below: Click or tap here to enter text. Assigned to: Click or tap here to enter text. Deadline: Click or tap to enter a date.	☐ Additional staff work required as noted below: Click or tap here to enter text. Assigned to: Click or tap here to enter text. Deadline: Click or tap to enter a date.

Recoverable Signature

X Timothy Bott

3/1/2019

State Chief Information Officer

Signed by: tbottenfield@mt.gov

POLICY AND OPERATIONS DECISION BRIEF

Complete this section for policy, process, standards or procedure decision briefs.

Problem Statement:

No auto forwarding of mt.gov emails to email accounts that are not mt.gov boxes.

- MATICTeamCalendar@mt.gov processes a rule to redirect content to: MATIC@DOJHLNITSD647.mtdoj.ads
- DOJDMOD@mt.gov processes a rule to redirect content to: DOJMod@justice.mtdoj.ads
- lscanconnectionlist@mt.gov processes a rule to redirect content to: lscanconnection@justice.mtdoj.ads
- dojlscanaa@mt.gov processes a rule to redirect content to: dojlivescanaa@justice.mtdoj.ad

Factors bearing on the problem:

Each of these email accounts are for correspondence between the DOJ and local law enforcement offices. This allows them to communicate to a common location (Share Point) that allows multiple DOJ IT teams to look over the information, without us having to grant and setup access to shared email boxes.

We use SharePoint as a common location for various law enforcement agency information that needs to be shared among different groups throughout DOJ IT and DOJ Criminal Investigation Division. It would place a large burden on the department to come up with another solution to share this information effectively with law enforcement agencies throughout the state. We have done this for another email account at DOJ MI Reconciliation dojmireconciliation@mt.gov to MIreconciliation@justice.mtdoj.ads.

Discussion:

Joe Frohlich's Notes: I have spoken to exchange team and they feel that since this is forwarding from on-prem exchange to on-prem SharePoint this is not an issue or a security risk. The SharePoint team might have a better solution. DOJ did ask for an exception to the Information Security Policy, which I changed to the POL-Electronic Mail Policy.

Conclusion:

Check the "Yes" box to approve this exception for one year ending March 1, 2020.

SERVICE CATALOG DECISION BRIEF

Complete this section for changes to the service catalog related to new, retired or changed (e.g. rates, enterprise) services.

Financial Implications:

This paragraph summarizes the financial impact of the proposed new service or change to existing service.

Describe the proposed service or change to the service:

This paragraph summarizes the proposed new service or change to existing service.

SITSD Resource Requirements:

What are the estimated SITSD resource requirements? (Staff, training, budget, procurement, project, technical needs, etc.)

Cost Recovery:

What are the costs of this proposal and how will costs be recovered? (Estimate rates and FTM considerations-final rate development will occur per approval of this request).

Recommendation

Tell the reader the action necessary to implement the service or change. This should be complete so the approver (CIO, Deputy CIO, or Director) only needs to sign to make the solution happen.

MANAGEMENT TEAM **REVIEW/COMMENT**					
	Comments	**Yes**	**No**	**NA**	**Date**
Application Technology Services Bureau	Audrey Hinman	☒	□	□	2/21/2019
Attorney	Click or tap here to enter text.	□	□	□	Click or tap to enter a date.
Business and Communications Coordinator	Click or tap here to enter text.	☒	□	□	2/18/2019
Chief Information Security Officer	Andy Hanks	☒	□	□	2/20/2019
Chief Technology Officer	Matt Van Syckle	☒	□	□	2/19/2019
Chief Financial Officer	Click or tap here to enter text.	□	□	□	Click or tap to enter a date.
Enterprise Support Bureau	Click or tap here to enter text.	□	□	□	Click or tap to enter a date.
Enterprise Technology Services Bureau Network	Click or tap here to enter text.	□	□	□	Click or tap to enter a date.
Network Technology Services Bureau	Click or tap here to enter text.	□	□	□	Click or tap to enter a date.
Office of Executive Services and Support	Rian Miller	☒	□	□	2/19/2019
Office of Contracts and Asset Management	Click or tap here to enter text.	☒	□	□	2/20/2019
Office of Finance and Budget	Click or tap here to enter text.	□	□	□	Click or tap to enter a date.
Public Safety Communications Bureau	Quinn Ness	☒	□	□	2/21/2019

MONTANA SITSD

STATE OF MONTANA
Department of Administration
State Information Technology Services Division

March 1, 2019

Tim Fox, Director
Department of Justice
PO Box 201401
Helena, MT 59620-1401

RE: Matt Grimm from DOJ submitted an exception request to the POL-Electronic Mail Policy to re-direct emails from mt.gov's accounts to non-state email addresses

Director Fox,

Matt Grimm submitted a policy exception request to allow DOJ mt.gov domain email accounts listed in the exception to forward email to a DOJ Microsoft SharePoint site. I had DOAs Security Services team conduct a security review, since this SharePoint site data is kept in our State Data Center the risk are minimal.

I am approving this exception request for one year ending March 1, 2020.

Please contact me if you have any questions.

Sincerely,

Timothy Bott

Tim Bottenfield
State Chief Information Officer

CC: Christie Magill, Communications Specialist, SITSD
Matt Grimm
Joe Frohlich

Montana Operations Manual ***Policy***	Category	**Communications and Networking, Information Technology**
	Effective Date	**11/01/2002**
	Last Revised	**6/30/2011**
Issuing Authority	**Department of Administration** **State Information Technology Services Division**	

POL-Electronic Mail Policy

I. Purpose

The purpose of this Policy is to implement the Electronic Mail Policy for defining actions to fulfill the responsibility.

II. Scope

This policy applies to all state agencies. 2-17-505 et seq., MCA, with the exemptions as defined in 2-17-516, MCA and 2-17-546, MCA.

III. Roles and Responsibilities

Roles and responsibilities are required by this policy and in accordance with POL-Information Security Policy - Appendix B (Security Roles and Responsibilities).

IV. Requirements

The State provided electronic mail (email) system must be used for: the conduct of state and local government business and delivery of government services; transmitting and sharing of information among governmental, research, and educational organizations; supporting open research and education in and between national and international research and instructional institutions; communicating and exchanging professional information; encouraging debate of issues in a specific field of expertise; applying for or administering grants or contracts; announcing requests for proposals and bids; announcing new services for use in research or instruction; and conducting other appropriate State business.

State employees shall use the state provided email system for state business purposes unless they do not have a direct connection to SummitNet. Qualifying employee's use of an external email system must be approved by SITSD. Employees shall use standard naming conventions for their email address when using an external email system.

All messages created, sent or retrieved, over the State's systems are the property of the State of Montana. Privacy of email is not guaranteed. Employees may not expect privacy for any messages. Agency System Administrators, management, and Department of Administration personnel may monitor email for performance, troubleshooting purposes or if abuses are suspected. By default, email is not a secure method of communication. Employees shall use their best judgment in sending confidential messages over the email system according to the POL-Information Security Policy and Data Classification Policy. The use of encryption must be considered when sending Data Classification Level 2 or Level 3 via electronic mail. It is highly recommended to use Montana File Transfer Service (Secure FTP) rather than email to share Data Classification Levels 2 or Level 3.

Employees shall attend email training. For additional help with using email, the

System Administrator shall be contacted.

Stationery may be used when it enhances the business content of email. Stationery, moving graphics or audio objects may not be used unnecessarily since they consume more resources such as disk space, network bandwidth and tend to detract from the message content.

Unsolicited email or spam, must be forwarded to email address: ServiceDesk@mt.gov for investigation before it is opened.

SITSD shall block email that is malicious in nature. As SITSD receives intel from various trusted third-party resources, the information may be used to create filters based on email addresses, subject line or content, where applicable, as a result of the threat involved. These requests must originate from the SITSD Security Office and may be implemented without executive-level approval.

Citizens have a Constitutional right to be able to communicate with the State of Montana. As a result, email addresses may not be blocked unless the sender is attempting to deliver malicious payloads, suspicious links or create a denial-of-service on the email system that may adversely affect the business operations of the State. The State of Montana may not arbitrarily block citizen’s email addresses unless one of the above conditions is met.

This policy applies to personal computers, other computing devices, and accessory equipment that store electronic data, information, and software programs.

A. Misuse Of Email

The following items represent, but are not restricted to, misuse of State email resources:

1. Circulating chain letters

2. Using the State email system for: 1) "for-profit" activities; 2) "non-profit" or public, professional or service organization activities that are not related to an employee's job duties; or 3) for extensive use for private, recreational or personal activities.

3. Statewide distributions of email. The system administrator should be contacted for correct procedures for large email distributions.

4. Using personal email accounts, such as Hotmail, outside of the State provided email system unless an exception has been granted.

5. Other misuse activities as referenced in the POL-Information Security Policy - Appendix A (Baseline Security Controls)

B. Guidelines - Recommendations, Not Requirements

1. Employees may check their mail with a frequency appropriate to their job duties and their departmental policy. If employees are unable to check their mail for an extended period of time, they may use the "auto reply" feature or make arrangements to have their mail picked up by someone else (supervisor, secretary, coworker) and reviewed to see if messages require a response.

2. If employees have a personal mailing list they feel would benefit the agency, they are encouraged to inform their System Administrator for the possibility of creating a public mailing list. Employees shall use care and discretion when sending email to mailing lists and/or large groups. Sending a large file to multiple recipients could severely impact the network.

3. The chance of receiving a virus increases with the use of email. Many viruses come embedded in attachments. Suspicious email messages must be forwarded to the State Information Security Manager for investigation before they are opened.

4. Employees may make judicious use of the features that increase email traffic and should strive to keep message and attachment sizes as small as possible. Use of graphics in auto-signatures or other parts of messages or attachments must be avoided because they greatly increase the size of a message. Use of the email text editor for simple messaging tasks is preferred since the same message created in a word processor is much larger. All attachments over one megabyte may be compressed (zipped) prior to sending.

5. Employees may use the junk email feature to classify spam email that gets past the enterprise email filters. Employees shall use this feature with caution to ensure valid email is not accidentally targeted as spam.

6. All entities that use the State's network that are not included within the scope of this policy are encouraged to adopt a similar policy.

7. Communications sent or received via email are "documents" under Montana Constitution Article II, section 9, or “public information” as defined in Section 2-6-1021, MCA, and as such, are available to the public (2-6-1003, MCA). Not all documents or public information are considered a “public record” (also defined in 2-6-1002, MCA). The determining factor in whether public

information is a public record is if it is “designated for retention.” Employees shall adhere to the requirements of GS3 when deciding whether to delete items from their email account. If an email needs to be retained, it may be moved to an archive folder or printed. Email placed in an employee's archive are the employee's responsibility. Retention of an email must be reevaluated when it has reached its retention time. Employees may contact the State Records Manager with any questions on retention schedules.

8. Email communication must resemble typical professional and respectful business correspondence. When drafting an email message, employees may not include anything they are not prepared for the public to read. Any communication may potentially become a basis for litigation and/or civil or criminal liability.

V. Definitions

Refer to the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms for common information systems security-related definitions

VI. Enforcement

A. PRO-Establishing and Implementing Statewide IT Policies, Standards, and Procedures governs policy changes or exceptions. Submit an Action Request form to request a review or change to this instrument. Submit an Exception Request form to request an exception. Changes to policies, standards, and procedures will be prioritized and acted on based on impact and need.

B. 2-17-514, MCA, addresses agency level enforcement information.

C. Montana Operations Manual (MOM) Discipline Policy addresses individual level enforcement information

VII. References

A. Legislation

1. Section 2-6-1002, MCA
2. Section 2-6-1003, MCA
3. Section 2-15-112, MCA
4. Section 2-15-114, MCA
5. Section 2-17-505, MCA
6. Section 2-17-511, MCA
7. Section 2-17-512, MCA
8. Section 2-17-514, MCA
9. Section 2-17-516, MCA
10. Section 2-17-546, MCA
11. Montana Information Technology Act (MITA), Sections 2-17-504 et seq., MCA

12. Article II, Section 9, of the Montana Constitution

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

1. Administrative Rules of Montana (ARM): ARM 2.12
2. NIST: Glossary of Key Information Security Terms
3. Statewide Policy: Discipline Policy
4. Statewide Policy: POL-Information Security Policy - Appendix B (Security Roles and Responsibilities)
5. Statewide Procedure: PRO-Action and Exception Request Procedure
6. Statewide Procedure: PRO-Establishing and Implementing Statewide IT Policies, Standards, and Procedures
7. State of Montana Office of the Governor Executive Order No. 09-2016
8. Secretary of State's General Schedule (GS)3

Catalog Task

Number	SCTASK0015801	**Opened**	01-17-2019 03:53:01 PM
Request	REQ0015238	**Opened by**	Matthew Grimm
Request item	RITM0015452	**State**	Work in Progress
Requested for	Matthew Grimm	**Due date**	01-17-2019 03:53:01 PM
Configuration item		**Assignment group**	Policy
Location		**Assigned to**	Christie Magill

Short description Policy Instrument Exception Request Form submitted by Matthew Grimm(DOJ)

Description:

Please fulfill this policy instrument exception request.

Related Attachments

Table name in sc_request, sc_req_item, sc_task AND Table sys ID in 313907b9db0f2b00c0a8365e7c961911, b13907b9db0f2b00c0a8365e7c961911, ca3907b9db0f2b00c0a8365e7c961933

0 Attachments

File name	Content type	Table name	Table sys ID

Notes

Work notes list

Work notes (Internal Only):

Activity

01-23-2019 08:35:56 AM **Christie Magill** - Changed: Assigned to, State

Assigned to: Christie Magill

State: Work in Progress was: Open

01-17-2019 03:53:01 PM **Matthew Grimm** - Changed: Impact, Opened by, Priority, State

Impact: 3 - Low

Opened by: Matthew Grimm

Priority: 4 - Low

State: Open

Details

Variables

Subject:

Email Fowarding Exemption to DOJ SharePoint

Organization:

Dept. of Justice

Contact:

Matthew Grimm

Phone:

406-444-3619

Email:

MGrimm@mt.gov

Date (or Timeframe) Needed:

Before 1/24/2019

Please provide detailed information below. The information may be refined throughout the request process.

1. Exception from Requirement: Which requirement of what policy, standard, rule, procedure, specification, etc. is the subject of this request?

No auto forwarding of mt.gov emails to email accounts that are not mt.gov boxes.

- MATICTeamCalendar@mt.gov processes a rule to redirect content to: MATIC@DOJHLNITSD647.mtdoj.ads
- DOJDMOD@mt.gov processes a rule to redirect content to: DOJMod@justice.mtdoj.ads
- lscanconnectionlist@mt.gov processes a rule to redirect content to: lscanconnection@justice.mtdoj.ads
- dojlscanaa@mt.gov processes a rule to redirect content to: dojlivescanaa@justice.mtdoj.ads

2. Business Requirement(s): Identify the requesting organization's affected business requirement(s) and how the requested exception affects the business requirement(s).

Each of these email accounts are for correspondence between the DOJ and local law enforcement offices. This allows them to communicate to a common location (Share Point) that allows multiple DOJ IT teams to look over the information, without us having to grant and setup access to shared email boxes.

3. Rationale of the Exception: Provide a business description and rationale for the requested exception.

We use SharePoint as a common location for various law enforcement agency information that needs to be shared among different groups throughout DOJ IT and DOJ Criminal Investigation Division.

4. Impact: What is the impact to the organization and the enterprise if the exception is granted, and if not

granted? (Strategic, operational, tactical, financial, etc.)

Would place a large burden on the department to come up with another solution to share this information effectively with law enforcement agencies throughout the state.

5. Other Considerations: Describe any other impact or considerations pertinent to the decision to approve an exception.

None known. We have done this for another email account.
DOJ MI Reconciliation
dojmireconciliation@mt.gov to
MIreconciliation@justice.mtdoj.ads

Task SLAs **Task = SCTASK0015801**

0 Task SLAs

SLA definition	Type	Target	Stage	Business time left	Business elapsed time	Business elapsed percentage	Start time	Stop time

No records to display

Approvers **Approval for = SCTASK0015801**

0 Approvals

State	Approver	Comments	Short description	Created

No records to display

Group approvals **Parent = SCTASK0015801**

0 Group approvals

Approval	Assignment group	Approval user	Short description

No records to display