UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-10

INFORMATION SECURITY POLICY

1   General Information:

- Statutory References: WV. Code § 18 B-1-6
- Passage Date: September 12, 2019
- Effective Date: October 15, 2019
- Updated Date: February 20, 2025

1.2. Scope:

This Policy applies to all faculty, ~~staff~~staff, and third-party Agents of Marshall~~the~~ University as well as any other University ~~affiliate~~agents who are authorized to access Institutional Data.

1.3. Background:

Marshall University ("University") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, ~~integrity~~integrity, and availability of Institutional Data as well as any Information Systems that store, ~~process~~process, or transmit Institutional Data.

2   Definitions:

2.1. "Agent" For the purpose of this Policy, is defined as any third-party that has been contracted by the University to provide a set of services and ~~who~~ stores, ~~processes or~~processes or transmits Institutional Data as part of those services.

2.2. ~~University Information Technology Council ("ITC") The official university committee advising university wide policy for Information Technology Resources usage at Marshall University. The council will create subcommittees as needed, with membership beyond itself to facilitate its work.~~

2.3.2.2.   "Information System" is defined as any electronic system that stores, processes, or transmits information.

2.3. "Institutional Data" is defined as any data that is owned or licensed by the University, or its agent.

~~2.4.~~

~~1~~3 **Policy:**

~~1.1~~3.1.   Throughout its lifecycle, all Institutional Data shall be protected in a manner that is ~~consistent with the Guideline for Data Classification~~ ~~considered reasonable and appropriate, as defined in documentation approved by the CIO and maintained by the Information Security Officer,~~ given the level of sensitivity, value and criticality that the Institutional Data has to the University ~~and its agents.~~ Any Technology Resource~~s~~ that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate according to the ~~ITG 4~~ Guideline for Data Classification.

~~1.2~~3.2.   Individuals who are authorized to access Institutional Data shall adhere to the ~~administrative procedure ITP 27~~ Information Security Roles and Responsibilities, as defined in ~~documentation approved by the CIO and maintained by the Information Security Officer.~~ this document.

~~1.3~~   ~~Maintenance:~~

3.3. This Policy will be reviewed by the University's Information Security Office on an annual basis or as deemed appropriate based on changes in technology or regulatory requirements.

3.4. Some violations of this Policy may occur unknowingly and will be addressed in collaboration with MUIT and the employee. However, serious or repeated violations of this Policy may result in restricted or revoked access to Institutional Data and University-owned Information Systems. In cases of extreme or willful misconduct, further administrative actions may be taken, up to and including termination of employment or contractor status, in accordance with existing policies and procedures. In certain situations, civil or legal consequences may also apply.

~~1.4~~   ~~Enforcement:~~
~~Violations of this Policy may result in suspension or loss of the violator's use of or privileges to Institutional Data and University-owned Information~~

~~Violations of this Policy may result in further investigation. Wi~~Systems. Additional ~~administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal, and equitable remedies may apply.~~

~~1.5~~   ~~Exceptions:~~
~~Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the Chief Information Officer and formally~~

3.5. Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the Chief Information Officer and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Formatted: Font: 12 pt, Not Bold, Condensed by 0.1 pt

Formatted: Normal, No bullets or numbering

Formatted: Font: 12 pt, Bold, Not Expanded by / Condensed by

Formatted: List Paragraph, Space Before: 0 pt, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: 0.38", Left + Not at 0.25"

Formatted: Font: Not Bold, Condensed by 0.1 pt

Formatted: Font: 12 pt, Condensed by 0.1 pt,

Formatted [4]

Formatted [5]

Formatted [6]

Formatted: Condensed by 0.1 pt

Formatted [7]

Formatted [8]

Formatted [9]

Formatted [10]

Formatted [11]

Formatted: Condensed by 0.1 pt

Formatted [12]

Formatted: Highlight

Formatted [13]

Formatted: Highlight

Formatted [14]

Formatted [15]

Formatted [16]

Formatted: Condensed by 0.1 pt

Formatted [17]

Formatted [18]

4 Information Security Roles and Responsibilities

4.1. Chief Information Officer

The Chief Information Officer (CIO) is a senior-level executive responsible for the overall technology strategy and implementation at the University. Responsibilities of the CIO include the following:

- Developing and implementing the University's IT strategy to support the institution's goals and objectives.

- Overseeing the management of IT infrastructure, including hardware, software, networks, and data centers.

- Ensuring the reliability, security, and scalability of the University's IT systems.

- Evaluating and implementing new technologies to improve efficiency and effectiveness.

- Ensuring compliance with relevant regulations and standards related to IT and data management.

- Developing and maintaining relationships with external vendors and partners.

4.2. Chief Information Security Officer

The Chief Information Security Officer (CISO) is a senior-level employee of the University who oversees the University's information security program. Responsibilities of the CISO include the following:

- Developing and implementing a university-wide information security program.

- Documenting and disseminating information security policies and procedures.

- Coordinating the development and implementation of a university-wide information security training and awareness program.

- Coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of Institutional Data.

3

4.3. Chief Data Officer

The Chief Data Officer (CDO) is a senior-level executive responsible for the governance and utilization of data as a strategic asset at the University. Responsibilities of the CDO include the following:

- Developing and implementing a data governance framework to ensure the quality, integrity, and security of Institutional Data.
- Overseeing data management practices and ensuring that data is used effectively across the University.
- Establishing data policies and standards to guide data collection, storage, processing, and usage.
- Ensuring compliance with data-related regulations and standards, including privacy laws and data protection regulations.
- Leading the data management team and coordinating with Data Stewards and Data Custodians.
- Identifying opportunities for data integration and analytics to enhance the University's operations and services.

4.4. Data Steward

A Data Steward is a senior-level employee of the University who oversees the lifecycle of one or more sets of Institutional Data. Responsibilities of the Data Steward include the following:

- Assign appropriate classification to Institutional Data by its sensitivity, value, and criticality of the University as defined by the Guidelines for Data Classification.
- Assign day-to-day administrative and operational responsibilities for Institutional Data to Data Custodians.
- Approve standards and procedures related to the day-to-day operational management of Institutional Data.
- Determine the appropriate criteria for obtaining access to Institutional Data. Provisioning access is the responsibility of the Data Custodian, or the assigned Data Steward based on the business function or support role.
- Ensure that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of Institutional Data.

- Understand and approve how Institutional Data is stored, processed, and transmitted by the University and/or third-party agents of the University.

- Define risk tolerances and accept or reject related security threats that impact the confidentiality, integrity, and availability of Institutional Data.

- Understand legal obligations and cost of non-compliance of data protections.

- Understand how Institutional Data is governed by university policies, State and Federal Regulations, Contracts, and other binding agreements.

4.5. Data Custodian

 A Data Custodian is an employee of the University who has dministrativeadministrative and/or operational responsibility to oversee Institutional Data. In many cases, there will be multiple Data Custodians. Data Custodian responsibilities are responsible for the following:

- Understand and report on how Institutional Data is stored, processed, and transmitted by the University, its agents, and third-party agenda of the University.

- Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of Institutional Data.

- Document and disseminate administrative and operational procedures to ensure consistent storage, retention, processing, and transmission of Institutional Data.

- Provision and deprovision access to Institutional Data as authorized by the Data Steward.

- Understand and report security risks and how they impact the confidentiality, integrity, and availability of Institutional Data.

4.6. Users

Users are any employee, contractor, agent, or third-party agent of the University who has authorized access to University Systems and/or Institutional Data. A user is responsible for the following:

- Adhere to policies, guidelines, and procedures pertaining to the protection of Institutional Data.

- Report suspected vulnerabilities in the confidentiality, integrity, or availability of Institutional Data to the Information Security office.

5 Information Security Awareness & Training

Any user with an account at Marshall University must complete the following annual information security trainings. Failure to complete these trainings may include disruption to your university account and/or termination of your university account.

- General Information Security Awareness Training (mandatory for all), including Phishing Awareness and FERPA training.

- GLBA Training (mandatory for any working with student financial accounts)

- HIPAA Training (mandatory for any working with Personal Health Information)

- PCI Training (mandatory for any working with payment card transactions)

6 Guidelines for Data Classification

Employees, agents, and third-party agents of Marshall University should be mindful and only utilize approved acceptable tools and services when storing, processing, and/or transmitting Institutional Data. Technology tools and services, even those at no cost to the University, must be reviewed according to ITP-3: Technology Governance and Procurement Review. This includes personal productivity technologies, including artificial intelligence (AI) tools, that process and retain data (i.e., meeting recording and transcription, large language models (LLMs), small language models (SLMs), image processors, etc.) If there are technology tools or services not listed in the Data Classification Guide, the CIO and the CISO should be notified via e-mail to vet through and information review and be approved accordingly. The Data Classification Guide will be reviewed and updated semi-annually by MUIT.

Table 6.1: Data Classification Guide

Type of Data	Description of Data	Examples of Data	Exposure Risk	Acceptable Tools & Services
Restricted	Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could	- Data protected by state or federal privacy regulations. (i.e., FERPA, HIPAA) - Data protected by confidentiality agreements. - Accounts Payable Information	High	- Blackboard LMS - Banner Student - Banner Finance - Banner HR

	cause a significant level of risk to the University or its agents.	- Bank Account Information - Employee Personnel Information - Student Loan/Financial Aid Information - Student Advising Information - Student Conduct Information - Enrollment Data - Student Health Data (i.e., Immunizations) - Donor Information - Building Utilities & Life Safety Information - Legal documents and litigation-related information - Network security information. - Critical infrastructure control systems information		- Banner Document Management - Dynamic Forms - OneDrive - Oracle Cloud Infrastructure (OCI) and associated data tables - MS Teams Files - SharePoint - E-Mail (only if ENCRYPT feature is used) - Qualtrics - Salesforce CRM - EAB Navigate - Exxat (Dietetics and Physical Therapy only) - Titanium (Speech and Hearing only) - Symplicity Advocate - StarRez (for the Landing only) - eResLife - Synchronizing files from OneDrive/MS Teams/Sharepoint to a Device is NOT ALLOWED for restricted data, unless device is encrypted. - PHI only allowable for M365, Titanium, and Exxat Software. - TouchNet Student Account Center, Advisor, e-Refunds
Private	Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its agents.	- By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. - University Budget Detail Information - Chart of Accounts & Ledger Information - Procurement Information & Contracts - Research Proposals & Grants	Medium	- All the above - E-Mail does NOT have to be encrypted for this data. - Synchronizing files between One Drive/MS Teams/SharePoint is

Formatted: List Paragraph, Space Before: 12 pt, After: 12 pt, Don't add space between paragraphs of the same style, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.25"

		- Limited Directory Information - Building Egress Plans - Room Utilization Data - Non-disclosure agreements (NDAs) and other contractual documents - Internal audit reports - Detailed IT infrastructure documents		permitted for Private information. - Adobe Express, Adobe Creative Cloud, Adobe Acrobat Pro DC - Copilot.Microsoft.com -
Public	Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its agents.	- Public Record Information - Press Releases - Course Information - Research Publications - General Directory Information - Campus Map - University policies and procedures that are publicly available. - Event announcements and community outreach information - Award and recognition information for faculty, staff, and students	Low	- No restrictions on storing or sending this type of data.

6.1. Guidelines for Storing, Processing, & Transmitting Restricted Information

As noted, restricted information is any data that when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its agents. The following provides best practices and guidelines for storing, processing, or transmitting restricted information:

- SharePoint sites must indicate visual cues of restricted information storage, access must be limited to only those with a need to know.

- Do not include restricted information in the subject line of a meeting or appointment on your calendar. Ensure the meeting details are protected via access controls or marked "Private."

- Do not download restricted information to a computing or mobile device unless device encryption is in place. Personally owned equipment and software should NEVER be used to process, store, or transmit restricted information.

- Do not share passwords. If you need to share or remember passwords, utilize a password management software approved by the Information Security Office.

- Do not leave paper copies of restricted information unattended. Ensure restricted information is

secured and shredded when no longer needed.

- Do not e-mail restricted information. Instead send a copy of the information via a secure, access-controlled link. Alternatively, utilize the "ENCRYPT" feature in e-mail to encrypt the transmission of the message.

- Do not use personal e-mail to conduct business or e-mail restricted information to a personal account.

- All systems storing restricted information must be reviewed and approved by the Information Security Office. Any systems storing, processing, or transmitted restricted information must utilize Multi-Factor Authentication standards (MFA).

- Keep in mind that FERPA and PHI is considered restricted information. Any data beyond "directory" level information should be considered restricted information. Note: MUID numbers, also known as "901" numbers are considered restricted information. For more information, visit FERPA – Consumer Information and Disclosures (marshall.edu).

- All university printers must be reviewed and approved by Marshall University Information Technology.

7 Technical Controls & Guidelines

7.1. VPN Access

VPN access provides users access to the University network and systems from a remote location. When connected to the university network (onsite or through VPN), information may be collected to ensure security and compliance. This information includes authentication attempts, device configuration compliance, unusual traffic patterns, duration of connection, latency, throughput, bandwidth utilization, and any anomalies.

VPN access will be audited, reviewed, and approved annually. VPN access is granted through the IT Service Desk, upon approval by an employee's direct supervisor and must meet the following requirements:

Multi-Factor Authentication (MFA) must be enabled

- the user's device is encrypted

- the user's device is registered for routine security updates, and has anti-malware software installed

- the user's device is a university managed device

To ensure optimal security when accessing the university network through VPN, the VPN connection will timeout after thirty (30) minutes of inactivity. Additionally, the maximum connection time of the VPN will be twelve (12) hours before reauthentication is required.

7.2. Device Administrative Access

In general, most users do not require administrative access to their university managed device. Device administrative access is granted through the IT Service Desk, upon approval by an employee's direct supervisor. Device administrative access is audited, reviewed, and approved annually.

7.3. Device Encryption

MUIT requires device encryption for any devices that have the potential to store restricted information, including FERPA and HIPAA data. Additionally, external file storage such as hard drives or USB drives must be approved by MUIT Information Security and encrypted when handling restricted information.

7.4. System Logging & Auditing

MUIT routinely collects logs on activities utilizing the University network. System logs will be retained for up to one year to ensure MUIT can conduct compliance reviews and investigations. MUIT also regularly monitors and analyzes log data to detect suspicious activities and identify potential security risks. Only authorized personnel in MUIT will have access to log data. Log data includes the following:

- Startup and shutdown events
- System errors and/or updates
- User activities including login attempts, file access, and changes to user permissions
- Network traffic information including source and destination IP Addresses, port numbers, and protocols
- Application logs including error messages, transaction records, and user activity
- Alerts and logs from security tools such as firewalls, intrusion detection systems, and endpoint detection software

7.5. Guest Accounts

Guest Accounts are provided to non-employees of Marshall University. Guest accounts require a university sponsor and will be audited, reviewed, and approved annually.

- Access to enterprise systems and Institutional Data must be approved by the employee's supervisor or guest account sponsor, as well as the Data Steward (or designee). Access to enterprise systems and Institutional Data will be audited, reviewed, and approved annually by the Data Steward (or designee) and the employee's supervisor or guest account sponsor.

- The University will participate in annual penetration testing to ensure the security of its information technology infrastructure and network. Any remediations will be coordinated by the Information Security Office and may include the participation and cooperation of other units and/or employees of the University.

- Marshall University Information Technology may collect and audit system transaction log files to detect and respond to security incidents in a timely manner. This may include user access, administrative actions, system errors, and security events.

7.6. Security Audits & Risk Assessments

MUIT participates in a variety of security audits and assessments. MUIT will routinely test and monitor the effectiveness of our technical safeguards through these assessments.

8   Vendor Risk Management

All technology systems or services used by the University, its agents, or third-party agents must undergo an information security review, as outlined in ITP-3: Technology Governance and Procurement Review. The Information Security Office utilizes the Higher Education Community Vendor Assessment Toolkit (HECVAT) provided by Educause to assess risk for technology vendors. The HECVAT is a questionnaire framework specifically designed for higher education to measure vendor risk. Elevated risk technologies or those that do not meet the standards herein must be approved by the Technology Executive Council, as well as the Chief Legal Counsel of the University.

9   Information Security Incident Response Procedure

9.1. Incident Definition:

An incident is the act of violating an explicit or implied security policy. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data resulting in an unwanted disruption or denial of service.

- the unauthorized use of a system for the processing or storage of data,

- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

All MU employees, agents, and third-party agents are required to report any activities that meet these incident criteria. It is our policy to keep any information specific to the incident confidential.

9.2. Incident Response Procedure:

- Step 1 - Information Security office and the IT Response Team is notified that a potential or actual breach has occurred through one of the following modalities: 1) IT Service Desk, 2) Direct Contact (i.e., Incident Response Form or e-mail abuse@marshall.edu), 3) Legal Counsel, Campus Police, or other Law Enforcement Agencies, 4) Internal/External Audit groups, 5) Human Resources, 6) External or Internal Complaints/Observations, etc.

- Step 2 – Determination of Severity

  Determination of the level of severity are as follows:

Severity	Symptoms
1	• Network or system outage with significant impact to the user population or operation of the University. • High probability of propagation. • Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.) • Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities. • Notification of entities outside the University is required.
2	• Some adverse impact to the operation of the University. • Adverse effects are localized or contained, or minimal risk of propagation. • No apparent release or compromise of sensitive data. • Remedial but not immediate action is required. • Notification of entities within the University is required.

3	• Minimal impact to small segment of user population or operation of university.
	• Completely localized, with few individuals affected, and presenting little or no risk to other entities.
	• No loss or compromise of sensitive data.
	• Remedial action is required.
	• Individual notification is required.

- Step 4 – Initial Notification of Incident: Based on the determined severity level, the following will receive an initial notification of the incident. All Severity 1 incidents require the formation of an Incident Response Team.

  o Severity 1: President, Chief of Staff, Chief Legal Counsel, Chief Information Officer, Chief Data Officer, Provost, Chief Financial Officer, Chief Marketing & Communications Officer, Chief of Police, others as determined.

  o Severity 2: Chief Legal Counsel, Chief Information Officer, Chief Data Officer, others as determined.

  o Severity 3: Chief Legal Counsel, Chief Information Officer, Chief Data Officer, others as determined. Notifications for this severity level will be sent post investigation.

- Step 5 – Investigation: The IT Information Security designate meets with the reporting organization or personnel to discuss and begin the investigation and documentation of the incident. The investigation proceeds as rapidly as possible to a highly probable conclusion of Severity Level. A preliminary report and Severity Level determination is provided to the Information Security within 48 hours. Investigation will include the following questions:

  o What happened?

  o What systems, devices, etc., were compromised?

14

- What is the net damage and costs?
- Was information lost or stolen? If yes, what?
- Was the information restricted or private?
- How was the information acquired?
- How was the system or device configured?
- What are the maintenance procedures?
- Do log files exist?
- Who was affected by the breach?

- Step 6: Determine level of external involvement needed included the following:
  - WV-BRIM
  - Law Enforcement
  - Cyber-Security consulting services
  - Others, as identified.
- Step 7: Documentation & Remediation will include the following processes:
  - Preservation of evidence
  - Determine root cause.
  - Implement required technology remediations.
  - File criminal charges (if required)
- Step 8: Develop & Implement Communication Plan for all notifications and media outreach.
  - Notification letters should contain the following: 1) a description of the breach, 2) Contact information for major credit reporting agencies, 3) recommendation to place a fraud alert on respective credit reports and ongoing monitoring, 4) a university contact for additional information.

15

- o Notifications of security incidents will be sent via first class mail on university letterhead to impacted individuals.

- o University Marketing and Communications will follow established policies and procedures for media relations and notifications.

- o All media inquiries or questions should be directed to the Chief Information Officer, Chief Information Security Officer, or a member of University Marketing & Communications.

2.3 • Step 9: Conclusion & Final Report; The Information Security Office will provide a final report to all identified stakeholders.

Page 1: [1] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [1] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [1] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [1] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [1] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [1] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [1] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [2] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [2] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 1: [3] Formatted	Penrod, Jodie	8/17/2024 9:08:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 2: [4] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Left, Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: 0.38", Left

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [5] Formatted	Penrod, Jodie	8/17/2024 9:09:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [6] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [6] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [6] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [6] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt, Highlight

Page 2: [7] Formatted	Penrod, Jodie	8/17/2024 9:05:00 PM

Heading 2, Space Before: 0 pt, No bullets or numbering, Tab stops: Not at 0.48"

Page 2: [8] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Font color: Auto, Condensed by 0.1 pt

Page 2: [9] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: 0.38", Left + Not

Page 2: [10] Formatted		

Font: 12 pt, Font color: Auto, Condensed by 0.1 pt

Page 2: [11] Formatted	Penrod, Jodie	2/18/2025 10:24:00 AM

Font: (Default) +Body (Calibri), 12 pt, Font color: Auto

Page 2: [11] Formatted	Penrod, Jodie	2/18/2025 10:24:00 AM

Font: (Default) +Body (Calibri), 12 pt, Font color: Auto

Page 2: [11] Formatted	Penrod, Jodie	2/18/2025 10:24:00 AM

Font: (Default) +Body (Calibri), 12 pt, Font color: Auto

Page 2: [11] Formatted	Penrod, Jodie	2/18/2025 10:24:00 AM

Font: (Default) +Body (Calibri), 12 pt, Font color: Auto

Page 2: [12] Formatted	Penrod, Jodie	8/17/2024 9:05:00 PM

Heading 2, Indent: Left: 0", Right: 0", Space Before: 0 pt, Line spacing: single

Page 2: [13] Formatted	Penrod, Jodie	8/17/2024 9:05:00 PM

Heading 2, Space Before: 0 pt, No bullets or numbering, Tab stops: Not at 0.48"

Page 2: [14] Formatted	Penrod, Jodie	8/17/2024 9:05:00 PM

Heading 2, Indent: Left: 0", Right: 0", Space Before: 0 pt, Line spacing: single

Page 2: [15] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Highlight

Page 2: [15] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Highlight

Page 2: [15] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Highlight

Page 2: [16] Formatted	Penrod, Jodie	8/17/2024 9:05:00 PM

Heading 2, No bullets or numbering, Tab stops: Not at 0.48"

Page 2: [17] Formatted	Penrod, Jodie	8/17/2024 9:05:00 PM

Heading 2, Indent: Left: 0", Right: 0", Space Before: 0 pt, Line spacing: single

Page 2: [18] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 2: [18] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 2: [18] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 2: [18] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 2: [18] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 2: [18] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt

Page 2: [18] Formatted	Penrod, Jodie	8/17/2024 9:10:00 PM

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Font: 12 pt, Condensed by 0.1 pt

Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

| Page 3: [20] Formatted | Penrod, Jodie | 8/4/2024 8:35:00 AM |

Bulleted + Level: 1 + Aligned at: 0.59" + Indent at: 0.84"

| Page 13: [21] Formatted | Penrod, Jodie | 8/4/2024 9:47:00 AM |

Font: 12 pt

| Page 13: [22] Formatted | Penrod, Jodie | 8/4/2024 9:47:00 AM |

Font: 12 pt

| Page 13: [23] Formatted | Penrod, Jodie | 8/4/2024 9:48:00 AM |

Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

| Page 13: [24] Formatted | Penrod, Jodie | 8/4/2024 9:48:00 AM |

Not Expanded by / Condensed by

| Page 13: [25] Formatted | Penrod, Jodie | 8/4/2024 9:48:00 AM |

Font: 12 pt

| Page 13: [26] Formatted | Penrod, Jodie | 8/4/2024 9:48:00 AM |

Not Expanded by / Condensed by

| Page 13: [27] Formatted | Penrod, Jodie | 8/4/2024 9:48:00 AM |

Font: 12 pt

| Page 13: [28] Formatted | Penrod, Jodie | 8/4/2024 9:49:00 AM |

Font: 12 pt

| Page 13: [29] Formatted | Penrod, Jodie | 8/4/2024 9:51:00 AM |

Not Expanded by / Condensed by

| Page 13: [30] Formatted | Penrod, Jodie | 8/4/2024 9:49:00 AM |

Right: 0.37", Line spacing: Multiple 1.08 li, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5", Tab stops: 0.58", Left

| Page 13: [31] Formatted | Penrod, Jodie | 8/4/2024 9:49:00 AM |

Font: 12 pt

| Page 13: [32] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Right: 0.37", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

| Page 13: [33] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 13: [34] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 13: [35] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 13: [36] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 13: [37] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

Page 13: [38] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [39] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [40] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [41] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [42] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [43] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [44] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [45] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [46] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [47] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [48] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Right: 0.37", Line spacing: Multiple 1.08 li

Page 13: [49] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [50] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [51] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 13: [52] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 14: [53] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 14: [53] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 14: [53] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 14: [53] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

| Page 14: [53] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [53] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [53] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [54] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [54] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [54] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [54] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [54] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [54] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [54] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [55] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [55] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [55] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [55] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [56] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [56] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [56] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

| Page 14: [57] Formatted | Penrod, Jodie | 8/4/2024 9:52:00 AM |

Not Expanded by / Condensed by

Page 14: [57] Formatted	Penrod, Jodie	8/4/2024 9:52:00 AM

Not Expanded by / Condensed by

Page 14: [58] Formatted	Penrod, Jodie	8/4/2024 9:54:00 AM

Font: 12 pt

Font: 12 pt

Page 14: [58] Formatted	Penrod, Jodie	8/4/2024 9:54:00 AM

Font: 12 pt

Page 14: [58] Formatted	Penrod, Jodie	8/4/2024 9:54:00 AM

Font: 12 pt

Page 14: [58] Formatted	Penrod, Jodie	8/4/2024 9:54:00 AM

Font: 12 pt

Page 14: [58] Formatted	Penrod, Jodie	8/4/2024 9:54:00 AM

Font: 12 pt

Page 14: [58] Formatted	Penrod, Jodie	8/4/2024 9:54:00 AM

Font: 12 pt

Page 14: [58] Formatted	Penrod, Jodie	8/4/2024 9:54:00 AM

Font: 12 pt

Page 14: [59] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [59] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 14: [60] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [61] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [62] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [63] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [63] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [63] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [63] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [63] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [64] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [65] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [66] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [66] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [66] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [66] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [66] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [66] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [66] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt, Not Expanded by / Condensed by

Page 15: [67] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt

Page 15: [67] Formatted	Penrod, Jodie	8/4/2024 9:47:00 AM

Font: 12 pt

Page 15: [68] Formatted	Penrod, Jodie	8/4/2024 10:00:00 AM

Font: 12 pt

Page 15: [68] Formatted	Penrod, Jodie	8/4/2024 10:00:00 AM

Font: 12 pt