Jefferson County Public Utility District
Risk Management Policy

Effective: DATE
Adopted Resolution: XXX

1.0 RISK MANAGEMENT POLICY

Risk is an inherent attribute of all utility activities. Risk is operationally defined as the probability that actions taken or not taken by utility employees will result in financial gain or loss. The objective of Jefferson County Public Utility District's (the District) risk management involves the continual identification of the District's exposure to accidental, contractual, legal, or regulatory losses.

The Risk Management Policy provides direction on the following topics:

1.01 General Risk Management Policy

It is the policy of the District that risks associated with the organization's operations will be proactively managed in a cost-effective and efficient manner consistent with prudent utility management practices. The District is committed to the highest standards of risk management. The Board, GM, and staff will comply with the guidelines set forth within the District's Risk Management Policy.

It is the intent of the District to protect itself against accidental loss or losses which affect personnel, property, assets, or the ability of the District to fulfill its mission. Actions to support this intent include the following:

1. Protecting against the consequences of losses that are catastrophic in nature;
2. Preserving District property, assets, and provided services;
3. Developing and maintaining a system that continually reexamines exposures, losses, and financing resources.

To achieve these objectives, the District utilizes risk management processes to minimize the probability and mitigate the effects of accidental losses at the most reasonable cost.

1.02 Risk Management Policy Adoption and Review

The Board is responsible for ensuring that the Risk Management Policy is up-to-date. To maintain effective and current guidance, the Board delegates responsibility to the GM to work with the appropriate staff members to review the Risk Management Policy on an annual basis. As necessary, the GM will coordinate with the Board to identify any necessary revisions that reflect:

- Changes in applicable legal and regulatory requirements
- Changes in the District's services and operations
- Changes in the District's risk management strategy or philosophy

The Risk Management Policy will be reviewed by the Board on an annual basis, and any subsequent amendments will be adopted by a majority vote of the Board.

2.0 INSURANCE

2.01 Insurance Coverage

It is the policy of the District to protect the organization against unpredictable loss through reasonable use of insurance and/or participation in risk pools. This policy is designed to establish processes to review and monitor the organization's insurance coverage.

In general, the District will ensure sufficient coverage when the risk is of a catastrophic nature or potentially beyond the capacity of the organization to absorb, or when it is required by law or contract. However, insurance will be limited to the availability of coverage at a reasonable cost, consistent with the probable frequency, severity, and impact of potential losses on the financial stability of the organization.

In specific, the District will maintain insurance or participate in an insurance pool for protect against risks related to the following areas:

- Crime
- Cyber Risk
- Excess Liability
    - Automobile
    - Community Service Activity
    - Emergency Assistance
    - Employer's Liability
    - Employment Practices
    - Failure to Supply
    - General
    - Joint Venture
    - Jones Act
    - Medical Malpractice Injury
    - Pollution
    - Standard Board Activity
- Property
- Public Officials Liability
- Wildfires
- Worker's Compensation

At the point of renewing any insurance contracts, the Board will collaborate with the GM to determine appropriate minimum coverage levels. This decision will be informed by the District's needs, comparison to data from peer agencies, industry trends, and recommendations from the insurer.

It is the current practice of the District to retain membership within the Public Utility Risk Management Services (PURMS). PURMS is a public entity risk pool organized on December 30, 1976 in the State of Washington under Revised Code of Washington (RCW) 54.16.200. It currently operates under RCW 48.62. Its members include the District, along with 17 other

public utility districts and NoaNet. The objectives of PURMS are to formulate, develop and administer a program of self-insurance in order to obtain lower costs for the various coverages provided to its members.

2.02 Insurance Monitoring and Reporting

The GM will share a summary of the District's insurance coverage with the Board on an annual basis for review and approval. If there are any significant changes to the District's insurance coverage, the GM will notify the Board within one week.

The Board also delegates to the GM the responsibility to develop a process by which any and all insurance providers will be promptly notified of significant changes to District operations or assets that may impact coverage.

3.0 POWER RISKS

3.01 Management of Power Supplier Relationships

It is the policy of the District that risks related to the acquisition and subsequent delivery of power will be mitigated through contract management, ongoing monitoring of the contracted power suppliers, and future consideration of the diversity of the energy portfolio.

It is the current practice of the District to acquire the majority of its energy supply through a power purchase contract with the Bonneville Power Administration (BPA). The District manages its energy delivery risks by ensuring that the contract with BPA—or any other third-party contracted with to provide energy—includes:

- Appropriate contractual penalties for non-delivery
- Appropriate insurance, including evidence of coverage

In addition, the District manages its exposure to energy supplies through involvement with peer organizations, such as the Public Power Council and the Washington PUD Association.

3.02 Power Supplier Monitoring

It is the policy of the District to monitor and mitigate risks related to third-party power suppliers by participating in working groups and advocacy coalitions. This is primarily accomplished through participation in the Public Power Council (PPC). The mission of the PPC is to preserve and enhance the benefits of the Federal Columbia River Power System (including the BPA) for consumer-owned utilities.

The Board should receive and review information from the PPC or similar groups on a biannual basis. The GM will be responsible for identifying and summarizing relevant information to share with the Board.

3.03 Future Energy Diversity

It is the policy of the District to explore the possibility of acquiring energy from a geographically and technologically diverse power suppliers and generating assets. As such, the District may consider diversity as one of the selection criteria when soliciting or renewing energy contracts.

3.04 Energy Delivery Risks

The District manages energy delivery risks by utilizing both in-house and BPA resources to perform load forecasting in line with standard utility practice.

As noted in the Insurance section, it is also the policy of the District to carry adequate insurance to protect against critical loss due to any issues related to providing power to customers (see 2.01 Insurance Coverage).

4. WATER RISKS

4.01 Water Regulatory Compliance

It is the policy of the District to maintain a set of processes to ensure that all water-related regulatory compliance requirements are met. Accordingly, the Board authorizes, delegates, and directs the GM to conform District operations to applicable regulatory standards for the provision of clean and safe water. As part of this work, the GM is responsible for documenting, auditing, and reporting on all mandatory compliance requirements, including regularly conducting water quality tests and annually producing the Consumer Confidence Reports on water quality testing results.

On a quarterly basis, the GM will report on the status of compliance with the application regulations to the Board.

As noted in the section 8.0 Regulatory and Legislative Risk Policy, the District will monitor new regulatory compliance requirements through participation in working groups and advocacy coalitions like the Washington Public Utility District Association (WPUDA).

4.02 Water Services Delivery Risks

It is the current practice of the District to source water through wells throughout East Jefferson County. To mitigate water service delivery risks, it the policy of the District to maintain a 10-year Water Plan to identify and determine sufficient water supply and infrastructure requirements to meet current and future needs.

As noted in the Insurance section, it is also the policy of the District to carry adequate insurance to protect against critical losses due to any issues related to providing water-related services to customers (see 2.01 Insurance Coverage).

5. BROADBAND RISKS

5.01 Broadband Services Delivery Risks

The District owns and operates a high-speed open-access fiber optic broadband network. In addition, through membership within the Northwest Open Access Network (NoaNet), the District owns a broadband network that is operated by NoaNet. Under Washington State law, the District is authorized to sell wholesale telecommunications services. Most of the major institutions within Jefferson County—including schools, government offices, medical facilities, and first responder buildings—are connected to the District's network.

Within this context, it is the policy of the District to maintain a set of processes to ensure that network outages and downtime are as limited as possible. The GM is responsible for determining appropriate procedures to reduce network outages and downtime. Activities may include, but are not limited to, maintaining agreements with broadband operators to monitor the network and respond within a specified timeframe to any disturbances.

As noted in the Insurance section, it is also the policy of the District to carry adequate insurance to protect against critical losses due to any issues related to providing broadband-related services to customers (see 2.01 Insurance Coverage).

6. CYBERSECURITY & IT SECURITY

Cybersecurity risks are those related to the probability of exposure or loss resulting from a cyber-attack or data breach within the District. Information Technology (IT) Security risks are those related to the probability of exposure or loss resulting from the misuse of IT systems, hardware, or software.

It is the policy of the District to monitor and mitigate cyber and IT-related risks by maintaining insurance for adequate protection against cybersecurity breaches (see 2.0 Insurance policy), ensuring that relevant policies are developed, implemented, and kept up-to-date, and supporting regular cybersecurity assessments.

The Board will delegate to the GM responsibility for ensuring that the District operates with policies in place that address the following areas:

Area	Minimum Scope
IT Governance	Policies in this area should minimally include guidelines for how the District makes strategic IT decisions related to projects and purchases, as well as IT hardware/software procurement and asset management guidelines.

IT and Cyber Security	Policies in this area should minimally cover information security (including employee roles and responsibilities, system access control, and password management), IT disaster recovery, IT/cyber incident response procedures.
IT Usage	Policies in this area should minimally include acceptable use guidelines for computers and phones used to complete District business that are owned by the company and/or employees.
Data Governance and Retention	Policies in this area should minimally include data storage, backup, and retention guidelines, data security and privacy practices, Payment Card Industry (PCI) compliance, and email retention guidelines.

Each policy will be reviewed and approved by the Board and will stipulate the frequency of review by the GM and Board.

In addition, the Board delegates to the GM the responsibility to conduct annual cybersecurity assessments.

In terms of communication, the GM will share a summary of the District's cybersecurity risks and general mitigation efforts with the Board on an annual basis for review and approval. If there are any significant cybersecurity breaches or attacks, the GM will notify the Board as soon as possible. In addition, the GM is responsible to share the results of any cybersecurity assessments, including proposed mitigation plans for any identified issues. Finally, the GM will share regular information about new technology initiatives, platforms, or third party vendors that may present cybersecurity risks to the Board for review and approval.

7. OPERATIONAL RISKS

Operational risk consists of the potential for failure of the District to act effectively to plan, execute and control organizational activities. Operational risk includes the potential for:

1. Organizational structure that is ineffective in addressing risk (i.e., the lack of sufficient authority to make and execute decisions, inadequate supervision, ineffective internal checks and balances, incomplete, inaccurate and untimely forecasts or reporting, failure to separate incompatible functions, etc.).
2. Absence, shortage, or loss of key personnel or lack of cross-functional training.
3. Lack or failure of facilities, equipment, systems, and tools such as computers, software, communications links and data services.
4. Exposure to litigation or sanctions resulting from activities like violating laws and regulations, not meeting contractual obligations, failing to address legal issues and/or receive competent legal advice, and not drafting and analyzing contracts effectively.
5. Errors or omissions in the conduct of daily operations, including activities like failing to execute transactions or violating guidelines and directives from the Board.

It is the policy of the District to monitor and mitigate operational risks through appropriate development and implementation of policies, performance of ongoing and timely internal and

external audits, and hiring a GM with sufficient expertise, skills, and integrity to adequately oversee the District's daily operations and staffing needs.

First, the Board manages operational risks by establishing a robust policy framework to guide operations. As such, the Board will ensure the District operates with policies in place that address the following areas, at minimum:

- 3- to 5-year strategic plan for the District
- Cybersecurity and IT security and governance (see 6.0 Cybersecurity & IT Security Policy)
- Emergency planning and disaster preparedness
- Employee and Board conduct, including conflict of interest, discrimination and harassment, retaliation/whistleblowing, and other ethical concerns
- Procurement and purchasing

Each policy will stipulate the frequency of review by the GM and/or Board.

Second, the Board manages operational risks by ensuring that the District performs ongoing and timely internal and external audits, as detailed in the District's Financial Policy.

Third, the Board manages operational risks by hiring and delegating to a GM with sufficient expertise, skills, and integrity to adequately oversee the District's daily operations and staffing needs. The GM shall propose changes to the District's Organizational Structure, as necessary to accomplish the District's Strategic goals, and submit said changes to the Board for final approval. It is the responsibility of the GM to ensure proper implementation of District resolutions, administrating directives, staffing policies and procurement procedures. In addition, the GM is responsible for hiring and terminating all employees, ensuring sufficient cross-training amongst staff so that critical functions are maintained without interruption that employees are aware of their responsibilities related to risk management.

8. REGULATORY & LEGISLATIVE RISKS

Regulatory risk encompasses risks associated with shifting state and federal regulatory policies, rules, and regulations that could negatively impact the District. Legislative risk is associated with actions by federal and state legislative bodies, such as any adverse changes or requirements that may infringe on the District's autonomy, increase its costs, impact its customer base, or otherwise negatively impact the District's ability to fulfill its mission.

It is the policy of the District to monitor and mitigate regulatory/legislative risk by participating in a variety of working groups and advocacy coalitions. This is primarily accomplished through membership in the Washington Public Utility District Association (WPUDA). WPUDA's main activities include:

- Representing PUDs in state, regional, and national legislative and policy processes.
- Providing information about PUDs and policy issues to its members and the public.
- Offering training and development programs for utility leaders.
- Providing opportunities for PUD leaders and staff to meet, share information, and plan cooperative activities.

In addition, the District Board and GM are responsible for regularly participating in regulatory rulemaking proceedings and legislative affairs to protect the District's interests.

9. SUSTAINABILITY RISKS

It is the policy of the District to recognize, monitor, and, where feasible, mitigate risks related to environmental sustainability and changes to the regional climate.

Sustainable energy is a core aspect of the District's mission. In addition, the District recognizes that changes in the regional climate have the capacity to create ongoing economic, social, and environmental risks. The primary potential impacts to District operations includes changes in streamflow that may impact hydroelectric generation, changes in energy consumption patterns, and increased threats from weather events.

While prioritizing the need for the District to remain financially viable, the Board delegates to the GM to pursue sustainability goals and activities that can help mitigate risks related to environmental changes, including:

- Continue the District's efforts to provide electric power that utilizes low-carbon, renewable resources to the extent possible and practical without impacting safety or reliability.
- Continue the District's efforts to educate and help the community conserve water and electrical resources.
- Continue efforts to reduce local carbon emissions as suggested in the Port Townsend-Jefferson County Climate Action Plan.
- Continue efforts to increase community resiliency by supporting local, renewable electricity and other technologies such as "demand response" and "smart grid."
- Participate in local, state, and regional efforts to encourage, develop and enact measures to mitigate carbon emissions in the energy sector that may contribute to climate change.

The GM is responsible for monitoring ongoing environmental, technical and economic trends transforming the utility industry. On an annual basis, the GM will present a summary of new trends and potential measures to prepare for and minimize the effects of environmental change that could impact the District's operations.

10. OTHER TYPES OF RISK MANAGEMENT

This Risk Management Policy is not intended to address the following types of risk, which are treated separately in other official policies, plans, and regulations of the District:

Risk Area	District Policy

Cybersecurity and information technology security and governance	Employee Handbook
Discrimination, harassment, and retaliation	Employee Handbook
Emergency planning and disaster response	Electric Emergency Plan, and Water Emergency Plan
Governance process, including role of the Commission and its Committees	Governance Policy
Internal controls	Financial Policy
Investments and financial exposure	Finance Policy
Procurement, purchasing, and contracting	Procurement Policy
Strategic planning	District Strategic Plan
Whistleblowing	Employee Handbook
Worker health and safety	Employee Handbook